STATISTICAL COMMUNICATION THEORY

Communication Theory Group
Department of Electrical Engineering
Northeastern University
360 Huntington Avenue
Boston, Massachusetts 02115

Contract No. AF19(628)-3312
Project No. 4610
Task No. 461003

This research was supported in part by the National Aeronautics and Space Administration under Grant NGR-22-011-013, Electronics Research Center, Cambridge, Massachusetts

FINAL REPORT

Period Covered: December 1, 1963 thru March 31, 1967

April 1967

Contract Monitor: Charles F. Hobbs, CRBK (Air Force)
Stephen J. O'Neill, ERC (NASA)

Distribution of this document is unlimited

Prepared
for

AIR FORCE CAMBRIDGE RESEARCH LABORATORIES
OFFICE OF AEROSPACE RESEARCH
UNITED STATES AIR FORCE
BEDFORD, MASSACHUSETTS

AFCRL-67-0272

Communication Theory Group Report No. 8

STATISTICAL COMMUNICATION THEORY

Communication Theory Group
Department of Electrical Engineering
Northeastern University
360 Huntington Avenue
Boston, Massachusetts 02115

Contract No. AF19(628)-3312
Project No. 4610
Task No. 461003

This research was supported in part by the National Aeronautics and Space Administration under Grant NGR-22-011-013, Electronics Research Center, Cambridge, Massachusetts

FINAL REPORT

Period Covered: December 1, 1963 thru March 31, 1967

April 1967

Contract Monitor: Charles F. Hobbs, CRBK

Prepared

for

AIR FORCE CAMBRIDGE RESEARCH LABORATORIES
OFFICE OF AEROSPACE RESEARCH
UNITED STATES AIR FORCE
BEDFORD, MASSACHUSETTS

PREFACE

This report is a summary and exposition of research efforts by the Communication Theory Group at Northeastern University during the period from December 1, 1963 to March 31, 1967, mainly under the Contract No. AF19(628)-3312. From September 1, 1965 to March 31, 1967, partial support has been received from NASA under the Grant No. NGR-22-011-013.

Over half of the studies have been presented as scientific reports, while the rest involves work which is still being pursued and extended. The former studies are summarized in part two and the latter are discussed in more detailed manner in part one. A list of publications is also attached.

The bulk of the research work lies in the area of coding and signal design for communication, for data transmission and for digitalized guidance control. A small part is devoted to associated problems such as optimum interpolation of sampled functions and optimum equalization of random channels.

Much of the work described in this Final Report is not considered closed. Research in these and related fields is being continued under Contract No. F19628-67-C-0112, which became effective on April 1, 1967.

ABSTRACT

This report describes four current research efforts: arithmetic codes, non-binary orthogonal codes, error-correcting schemes, and filtering of PAM signals for a randomly selected channel.

Seven Scientific Reports are summarized. The subject matter of these reports includes the following topics: linear product codes, detection of digital data, optimum interpolation of sampled functions, adaptive bandwidth compression, and the design and shaping of analog signals.

TABLE OF CONTENTS

		Page No.
PREFACE		i
ABSTRACT		ii
TABLE OF CONTENTS		iii
PART ONE - REPORT ON RECENT STUDIES		1
CHAPTER I	ARITHMETIC CODES	1
CHAPTER II	NON-BINARY ORTHOGONAL CODES	25
CHAPTER III	ERROR-COUNTING SCHEMES	41
CHAPTER IV	DATA TRANSMISSION BY PULSE AMPLITUDE MODULATION THROUGH A NOISY CHANNEL WHICH HAS BEEN RANDOMLY SELECTED	53
PART TWO - SUMMARY OF 7 SCIENTIFIC REPORTS		64
CHAPTER I	PULSE SHAPING BY MANIPULATING TRANSFORM ZEROS	64
CHAPTER II	PROPERTIES AND APPLICATION OF AUTOCORRELATION-INVARIANT FUNCTIONS	67
CHAPTER III	ORTHOGONAL SIGNALLING PULSES WITH THE SAME AUTOCORRELATION	69
CHAPTER IV	ON LINEAR PRODUCT CODES AND THEIR DUALS	72
CHAPTER V	IMPLEMENTATION AND PERFORMANCE OF THE MAXIMUM-LIKELIHOOD DETECTOR IN A CHANNEL WITH INTERSYMBOL INTERFERENCE	74
CHAPTER VI	OPTIMUM INTERPOLATION OF SAMPLED FUNCTIONS	77
CHAPTER VII	A STUDY OF ADAPTIVE BANDWIDTH COMPRESSION	81
LIST OF PUBLICATIONS		83

PART I REPORT ON RECENT STUDIES

CHAPTER I

ARITHMETIC CODES

N. T. Tsao-Wu and S. H. Chang

Introduction

Arithmetic codes, also denoted as AN codes and linear residue codes, are based on ordinary arithmetic operations. They are useful both in controlling computation errors in digital computer and in data transmission. They are practical in that encoding and decoding operations can be performed using general purpose computers. This class of codes was first investigated by Diamond[1] and Brown.[2] Their studies were followed by Peterson[3], Henderson[4], Berstein and Kim[5], Chien[6], Stein[7] and Mandelbaum.[8] Most of the results have been in the area of correcting and/or detecting burst errors. Recently, a class of linear residue codes that corrects random errors has been discovered independently by Mandelbaum*, Barrows[9], and this group.

In this chapter, after briefly stating some useful concepts in elementary Number Theory, we shall discuss a class of binary cyclic** arithmetic codes. An expression for the minimum distance of such codes is established and the result is extended to ternary codes. We then present attempts to calculate the minimum distances of a much more general class of arithmetic codes which

---

*Mandelbaum's paper and a discussion by Chang and Tsao-Wu are to appear in the IEEE Transactions on Information Theory.

**The non-zero code words form a cyclic multiplicative group.

correct multiple errors. Finally, bounds on the minimum redundancy for the burst-error-correcting arithmetic (Fire) code proposed by Mandelbaum are found.

Definition

Arithmetic codes are, in general, of the form AN + B, where N is the number to be coded and A and B are positive integers. It is a mapping of a set of integers $0,1,2,\ldots,n_i,\ldots$ into the set of integers $B, A+B, 2A+B,\ldots,An_i+B,\ldots$. Each of these integers, when represented in radix r number system, is a code word. In particular, when B = 0, for numbers $n_1, n_2,\ldots$, we have

$$An_1 + An_2 + \ldots = A(n_1 + n_2 + \ldots),$$

if $(n_1 + n_2 + \ldots)$ is also a number in the set under consideration. This implies that the sum of the coded numbers is the coded number of the sum and, in this sense, it is a linear code.

To recover the coded number, we first take the residue of the received number modulo A. It it is a non-zero residue, an error has occurred; if it is zero, there has been no error, or an undetectable error has occurred. This justifies the name, linear residue code.

The arithmetic weight W(A) of any number A is the least number of non-zero terms necessary to express A in the form

$$A = \sum c_j 2^j, \quad c_j = 0, \pm 1.$$

The arithmetic distance, $D(A_1, A_2)$, between any two numbers, A_1 and A_2, is defined to be the arithmetic weight of the magnitude of their difference; that is,

$$D(A_1, A_2) = W(|A_1 - A_2|).$$

Hereafter, the term weight or distance will mean arithmetic weight or arithmetic distance respectively, unless otherwise stated.

Some Basic Concepts from Number Theory[10,11]

(i) Principal Division Identity for the Integers

If a and b are integers, $b \neq 0$, then there are unique integers s and t such that $a = sb + t$ and $0 \leq t < b$.

(ii) Representation of a Number in Radix r

Let r be a positive integer greater than 1. Then each positive integer A can be expressed uniquely in the form

$$A = c_n r^n + c_{n-1} r^{n-1} + \cdots + c_1 r + c_o,$$

where $0 \leq c_i \leq r-1$ $(i = 0,1,\ldots,n-1)$ and $0 < c_n \leq r-1$.

(iii) Canonical Decomposition of a Number into a Product of Primes

Every integer $A(> 1)$ can be expressed as a product of primes and uniquely, if one disregards the ordering of primes, as

$$A = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

in which $p_1, p_2, \ldots, p_k$ are different primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive non-zero integers.

(iv) The Euler Function

The Euler function $\phi(A)$ is defined for all positive integers A and represents the number of numbers of the sequence $0,1,\ldots,A-1$ which are relatively prime to A. In terms of the canonical decomposition of the number A, it can be shown that

$$\phi(A) = A(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k}) = A \prod_{i=1}^{k} (1 - \frac{1}{p_i})$$

and in particular

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}, \quad \phi(p) = p-1.$$

(v) Congruence Relations

If a and b are integers, then $a \equiv b \pmod{m}$ means that (a-b) is divisible by m or that a is congruent to modulo m. In other words, there is an integer k such that $a-b = km$.

(a) Congruence classes (mod m) are members of a set $c_0, c_1, \ldots, c_{m-1}$ such that for each $R = 0,1,\ldots,m-1$, where R is called a residue, c_R consists of all the integers $km + R$, $k = 0, \pm 1, \pm 2, \ldots$.

(b) The set of these congruent classes (mod m) is a ring with respect to addition and multiplication. This ring is a field if and only if m is a prime.

(c) One can form a reduced system of residues, (mod m) by taking one residue from each class which contains numbers that are relatively prime to m; there are $\phi(m)$ in number.

(d) If a and m are relative prime, and x runs through a reduced system of residues modulo m, then ax also runs through a reduced system of residues modulo m.

(vi) The Theorems of Euler and Fermat

(a) For $m > 1$, a and m are relatively prime, we have

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

This is the Euler's theorem.

(b) If p is a prime, and a is not divisible by p, we have

$$a^{p-1} \equiv 1 \pmod{p}$$

or

$$a^{p} \equiv a \pmod{p}$$

for all integers a. This is the Fermat's theorem.

(vii) The Multiplicative Group G(A)

The set of all integers smaller than and relatively prime to a given integer A forms a commutative group G(A) with respect to multiplication modulo A

and, by (iv), there are $\phi(A)$ in number. Let $s \in G(A)$, and e be the smallest integer such that

$$s^e \equiv 1 (\text{mod } A),$$

then e is called the exponent of s mod A and is denoted by $e(s,A)$. It can be shown that, using notation in (iii)

$$e(s,A) = \text{LCM}\left[e(s,p_1^{\alpha_1}), e(s,p_2^{\alpha_2}),\ldots,e(s,p_k^{\alpha_k})\right].$$

In particular, if A is of the form p^m (i.e., a power of a prime), then there exists elements g in G(A) such that $e(g,p^m) = \phi(p^m)$, and they are called primitive elements. In addition, G(A) is a cyclic group in which g is called a generator, i.e., all the elements of G may be expressed as distinct powers of g.

The Binary Cyclic Arithmetic Code

Consider the AN code in which A is chosen such that

$$A = \frac{2^{B-1}-1}{B},$$

where B* is a prime with 2 as a primitive root. The binary expression for A (or A•1) can then be obtained from the periodically recurring sequence in the fractional expansion of B since

$$\frac{1}{B} = 0.\dot{a}_1 a_2 \ldots \dot{a}_{B-1}$$

$$A = 2^{B-1} \cdot \frac{1}{B} - \frac{1}{B} = a_1 a_2 \ldots a_{B-1} \cdot$$

*This B is distinct from the B of page 2.

This sequence is called the quotient-sequence.

Lemma 1

Each element of the quotient-sequence can be expressed in the form, $a_i = (2^i \bmod B) \bmod 2$.

Proof

From the decimal expansion of B, using 2 as radix, one gets, for $i \leq B-1$,

$$\frac{2^i}{B} = a_1 a_2 \cdots a_i \cdot a_{i+1} a_{i+2} \cdots a_{B-1} a_1 a_2 \cdots = q + \frac{2^i \bmod B}{B},$$

where q and $\frac{2^i \bmod B}{B}$ are the integer and the decimal part of the ratio. The integer part is

$$q = \frac{2^i}{B} - \frac{2^i \bmod B}{B} = a_1 a_2 \cdots a_i$$

or

$$2^i - 2^i \bmod B = (a_1 a_2 \cdots a_i)\, B.$$

Now, noting that B is an odd number, and taking congruences modulo 2 on both sides, we have

$$(2^i \bmod B) \bmod 2 = a_i.$$

There are B-1 non-zero code words expressing in binary digits the numbers AN, for $N = 1,2,\ldots,B-1$. All code words are B-1 digits long and are cyclic shifts of each other. That is, they are all of the form $A \cdot (2^i \bmod B)$. The all-zero code word is also added to the code giving a total of B code words.

Property of the Quotient-Sequence

(i) The first half of the sequence is the complement of the second half, digit by digit.

i.e., $$a_i + a_{i + \frac{B-1}{2}} = 1, \quad 1 \le i \le \frac{B-1}{2}$$

or $$\left(2^{\frac{B-1}{2}} + 1\right) A \equiv 0 \bmod \left(2^{B-1} - 1\right). \qquad (1)$$

Indeed if

$$B \text{ divides } (2^{B-1} - 1) \text{ and } B \text{ does not divide } \left(2^{\frac{B-1}{2}} - 1\right),$$

then

$$B \text{ must divide } \left(2^{\frac{B-1}{2}} + 1\right),$$

i.e.,

$$\left(2^{\frac{B-1}{2}} + 1\right)\left(\frac{2^{B-1} - 1}{B}\right) = m\left(2^{B-1} - 1\right), \ m \text{ an integer},$$

hence (1) is proved.

(ii) There are equal number of ones and zeros. This follows from (i), since (B-1) is even.

Theorem 2

For a cyclic AN code, where $A = \frac{2^{B-1}-1}{B}$, B is a prime greater than 3, the distance is given by

$$\left[\frac{B+1}{3}\right].^{*}$$

---

*[x] denotes the integer part of x.

Proof

Any prime $B > 3$ is congruent to either 1 or $2(\equiv -1)$ modulo 3, i.e.,

$$\text{either} \qquad x = \frac{B-1}{3}, \quad \text{an even integer}$$

$$\text{or} \qquad x = \frac{B+1}{3}, \quad \text{an even integer.}$$

We shall consider the first case only. The second case can be proved in a similar manner. Let $N_i = (2^i) \bmod B$. Without loss of generality we list A·1 and A·3 in the ordering of N_i rather than in the familiar ordering of i in Table I. We shall first show that, in general, the digits of A·3 differ from those of A·1 only within the central interval.

TABLE I

Intervals of N_i	I	II	III
$N_i = (2^i) \bmod B$	(1 2 ... x-1 x)	(x+1 x+2 ... 2x-1 2x)	(2x+1 2x+2 ... B-2 B-1)
A·1	(1 0 ... 1 0)	(1 0 ... 1 0)	(1 0 ... 1 0)
A·3	(Same)	(0 1 ... 0 1)	(Same)
A·3-A·1 = A·2	(0 ... 0)	(-1 +1 ...-1 +1)	(0 ... 0)

In the interval I, the digits of the sequence in A·3 remain the same as those in A·1 because both $3 \cdot [(2^i) \bmod B]$ and $(2^i) \bmod B$ are less than B. Therefore, in this interval

$$[(2^i) \bmod B] \bmod 2 = [(3 \cdot 2^i) \bmod B] \bmod 2.$$

This congruence is again satisfied in the interval III, where

$$2B < 3 \cdot [(2^i) \bmod B] < 3B.$$

However, in the interval II,

$$B < 3 \cdot [(2^i) \bmod B] < 2B,$$

the above congruence relation is no longer satisfied. It follows that the non-zero digits of A·2 occur over the interval II with a total number of x digits. For this number to be the minimum weight of A·2, it is sufficient to show that these digits are not pairwise adjacent in the ordering of i. In other words, it is sufficient to show that the following adjacency condition for any two numbers within this interval N_a and N_b, cannot be satisfied.

$$\begin{aligned} N_b - N_a &= (2^{i_b} \bmod B) - (2^{i_a} \bmod B) \\ &= (2^{i_a+1} \bmod B) - (2^{i_a} \bmod B) \\ &= 1 \cdot 2^{i_a} \bmod B = N_a , \end{aligned}$$

where we take $N_a > N_b$ and $i_b > i_a$ without loss of generality. This is evident from the fact that

$$N_b - N_a \leq x-1$$

while

$$x+1 \leq N_a \leq 2x.$$

Thus the minimum weight of A·2 is $x = \frac{B-1}{3}$. Other code words are cyclic shifts of A·2 (in minimum weight representation)

and have the same minimum weight.* The minimum distance of the code, is therefore, given by

$$x = \frac{B-1}{3}$$

or $$x = \frac{B+1}{3} \text{ for the second case.}$$

Combining, we have

$$x = \left[\frac{B+1}{3}\right] .$$

The code is capable of either (i) detecting x-1 random arithmetic errors or (ii) correcting $\frac{x-2}{2}$ and detecting $\frac{x-2}{2}$ + 1 random arithmetic errors.

Extension to the Ternary Cyclic Code

The ternary cyclic AN code is obtained by selecting $A = \frac{3^{B-1}-1}{B}$, where B is a prime, with 3 as a primitive root. The minimum distance in this case is found to be $2 \cdot \left[\frac{B+1}{4}\right]$. The proof is similar to the argument used for the binary case. Therefore, only the additional steps required in the proof will be stated in detail. We require some preliminary remarks to establish a result needed in proving the expression for the minimum distance, namely, those primes, having 3 as a primitive root, $B = 4x-1$ satisfy $B = 1 \bmod 3$ and those of the form $B = 4x+1$ must satisfy $B = 2 \bmod 3$.

*Note that half of the code words are represented by their negative complements in this mapping, i.e., $A \cdot N \longrightarrow A \cdot \{-(B-N)\}$.

Lemma 3

3 is a quadratic residue of B, if and only if

either $B \equiv 1 \bmod 3$ and $B \equiv 1 \bmod 4$

or $B \equiv 2 \bmod 3$ and $B \equiv 3 \bmod 4$.

An equivalent statement is that 3 is a quadratic residue of B if and only if the prime B is in the form of $12i \pm 1$, i being any real integer.

Proof

We make use of the definition of Legendre symbol and the quadratic Reciprocity Law in Number Theory. If $B = 12i \pm 1$,

$$\left(\frac{3}{B}\right) = \left(\frac{B}{3}\right)(-1)^{B-1/2} = \left(\frac{12i+1}{3}\right)(-1)^{12i/2} = \left(\frac{1}{3}\right) = 1.$$

If $B = 12i-1$,

$$\left(\frac{3}{B}\right) = \left(\frac{-1}{3}\right)(-1)^{(12i-2)/2} = (-1)^{(12i-2)/2}\,(-1)^{(12i-2)/2} = 1.$$

By definition of the Legendre symbol, 3 is a quadratic residue of B.

To show the converse, if 3 is a quadratic residue of B, one can show by exhausting all possible forms of B that only $B = 12i \pm 1$ satisfies

$$\left(\frac{3}{B}\right) = 1,$$

whilst $B = 5 \bmod 12$ and $B = 7 \bmod 12$ do not.

Lemma 4

If any prime B is of the form $12i \pm 1$, i being any real positive integer, then 3 cannot be its primitive root.

This follows immediately from the above lemma.

Lemma 5

Each element in the quotient-sequence can be represented in the form of $c(3^i \bmod B) \bmod 3$, where $c = 2$ when B is in the form $4x-1$ and $c = 1$ when B is in the form $4x+1$.

Proof

From the division algorithm, the i^{th} remainder of $\frac{1}{B}$ is given by $N_i = 3^i \bmod B$, or as a recursive relation

$$N_i = N_{i-1} \cdot 3 - a_i B$$

following in the same manner as in Lemma 1. It can be shown that

$$a_i = 2(3^i \bmod B) \bmod 3 \quad \text{for} \quad B = 4x-1$$

or

$$a_i = (3^i \bmod B) \bmod 3 \quad \text{for} \quad B = 4x+1.$$

Theorem 6

The distance of the ternary cyclic code, where $A = \frac{3^{B-1}-1}{B}$, is $2 \cdot \frac{B-1}{4}$ if $B = 4x+1$, and is $2 \cdot \frac{B+1}{4}$ if $B = 4x-1$.

Proof

We shall prove this theorem for the case $B = 4x+1$. It follows that $B = 2 \bmod 3$, $x = 1 \bmod 3$ and $a_i = (3^i \bmod B) \bmod 3$. We follow the general scheme as in Theorem 1 by listing $A \cdot 1$ and $A \cdot 4$ in the ordering of N_i, $N_i = 3^i \bmod B$, as shown in Table 2.

TABLE II

N_i	(1 2 3 ... x)	(x+1 x+2 ... 2x)	(2x+1 2x+2 ... 3x)	(3x+1 3x+2 ... 4x)
A•1	(1 2 0 ... 1)	(2 0 1 ... 2)	(0 1 2 ... 0)	(1 2 0 ... 1)
A•4	(No Change)	(0 1 2 ... 0)	(2 0 1 ... 2)	(No Change)
A•3	(0 0 ... 0)	($\bar{2}$ 1 1 ... $\bar{2}$)	(2 $\bar{1}$ $\bar{1}$ ... 2)	(0 0 ... 0)

By the same reasoning as in Theorem 2, we note that there are 2x non-zero terms for A•3 belonging to the interval $L = \{x+1,\ldots,2x\}$ and $M = \{2x+1,\ldots,3x\}$ and show that any number L_j in L and any number M_k in M cannot be adjacent in the ordering of i. Within the interval L, we only need to prove that the numbers with coefficients ± 2 are not adjacent in the ordering of i.

Let two such typical numbers be

$$L_1 = (x+1) + 3\ell_1 \qquad L_2 = (x+1) + 3\ell_2,$$
$$= 3^{i_1} \bmod B \qquad = 3^{i_2} \bmod B$$

in which ℓ_1, ℓ_2 are non-negative integers.

Without loss of generality, we assume $L_2 > L_1$, $i_2 > i_1$.

The adjacency relation in i requires that

$$L_2 - L_1 \equiv (3^{i_1+1} \bmod B) - (3^{i_1} \bmod B) \equiv 2L_1 \bmod B.$$

But

$$L_2 - L_1 = 3(\ell_2 - \ell_1) = 0 \bmod 3,$$

and $$2L_1 = 2(x+1) + 6\ell_1 = 1 \bmod 3.$$

Hence $L_2 - L_1$ is not congruent to $2 \cdot L_1$.

In a like manner, one can show that those in M with ± 2 as coefficients cannot be adjacent in the ordering of i.

Therefore, the weight of $A \cdot 3$ is given by

$$2 \cdot x = 2 \cdot \frac{B-1}{4},$$

which is also the distance of the code. For the case when $B = 4x-1$, we have a minimum distance equal to $2 \cdot \frac{B+1}{4}$.

A General Class of Multiple Random Error-Correcting Codes

It has been stated that any integer can be expressed as a product of prime, and in particular,

$$2^{B-1} - 1 = \left(2^{\frac{B-1}{2}} - 1\right)\left(2^{\frac{B-1}{2}} + 1\right)$$

$$= \left(2^{\frac{B-1}{2}} - 1\right)\prod_{i=1}^{k} p_i^{\alpha_i},$$

where B is a prime, with 2 as a primitive root. Since B must divide $\left(2^{\frac{B-1}{2}} + 1\right)$, it follows that one of the primes, p_i must be equal to B, with $\alpha_i = 1$. Without loss of generality, let $p_1 = B$ and $\alpha_1 = 1$. The generator A chosen for the binary cyclic code discussed in the previous section clearly is given by

$$A = \left(2^{\frac{B-1}{2}} - 1\right)\prod_{i=2}^{k} p_i^{\alpha_i}.$$

With such a choice of A, we have a cyclic* code, having B code words, including the all-zero code word.

Now choose A such that

$$A = \frac{\left(2^{\frac{B-1}{2}} - 1\right)\prod_{i=2}^{k} p_i^{\alpha_i}}{p_j^{\gamma_j}}$$

for some j, $2 \le j \le k$, $1 \le \gamma_j \le \alpha_j$.

This will result in a code having $B \cdot p_j^{\gamma_j}$ code words of code length (B-1), provided that $e(2,A) = B-1$ and which consists of disjoint cyclic subsets of code words. We can still call it a cyclic code, however, in the sense that any code word can always be obtained by cyclic-shifting some other code words. This is the practice in cyclic algebraic codes.

The determination of the minimum distance is no longer a simple matter since each cyclic subset must be examined. Referring to the notation already developed in the proof of Theorem 2, we note that the central interval of N_i was uninterrupted since 2 is a primitive root of B. Now, for the determination of the minimum distance of each subset, the central interval of

$$N_i = 2^i \bmod \left(B \cdot p_j^{\gamma_j}\right)$$

(which remains to play the important role of determining the minimum weight) is no longer uninterrupted. Thus the number of residues modulo $(B \cdot p_j^{\gamma_j})$ that fall within the central interval can be different for each subset, and it is

---

*It is cyclic in the strictest sense, that is, every code word can be obtained by cyclic-shifting any other code words.

this number that gives the minimum distance for the particular subset.

An algorithm is formulated to count the number of residues modulo $(B \cdot p_j^{\gamma_j})$ that fall within the central interval for each possible subset. However, when $p_j^{\gamma_j}$ becomes large, the counting process becomes a tedious one, even for a computer. The actual computation only counts for half of the word length since the other half is its complement, from the fact that A has the factor $\left(2^{\frac{B-1}{2}} - 1\right)$.

Fig. 1 is a plot of $\frac{k}{n/2}$ (transmission rate) versus $\frac{d}{2n}$ (the 'error' correctability rate) for various code lengths n = B-1. We use only half of the code length. Therefore, two code words are obtained from each original code word, one being the complement of the other. The minimum distance, d, of the original code word is also halved, but the ratio d/n remains unchanged. Also super-imposed on the same plot are the Hamming upper bound and Varsharmov-Gilbert bound for $n \to \infty$.

Burst Error Detection and Correction

For the cyclic code presented at the beginning of this chapter, we have the code word A·1 in its binary form

$$A \cdot 1 = a_1\, a_2 \cdots a_{B-1}\,, \quad a_i = 0,1.$$

As a result of generation, this code word begins with $[\log_2 B]^*$ zeros, and both $a_{[\log_2 B]+1}$ and a_{B-1} will be ones. Thus any error pattern of length $B-2-[\log_2 B]$ or less cannot be a code word, since it represents a number less than A. That is, for $e = 0\ 0 \ldots 0\ e_{[\log_2 B]+2} \cdots e_{B-2}\ e_{B-1}$ or its cyclic shifts, where $e_{[\log_2 B]+2}\,,\ e_{B-1} \neq 0$, then $e \not\equiv 0 \pmod{A}$ and the burst is detectable.

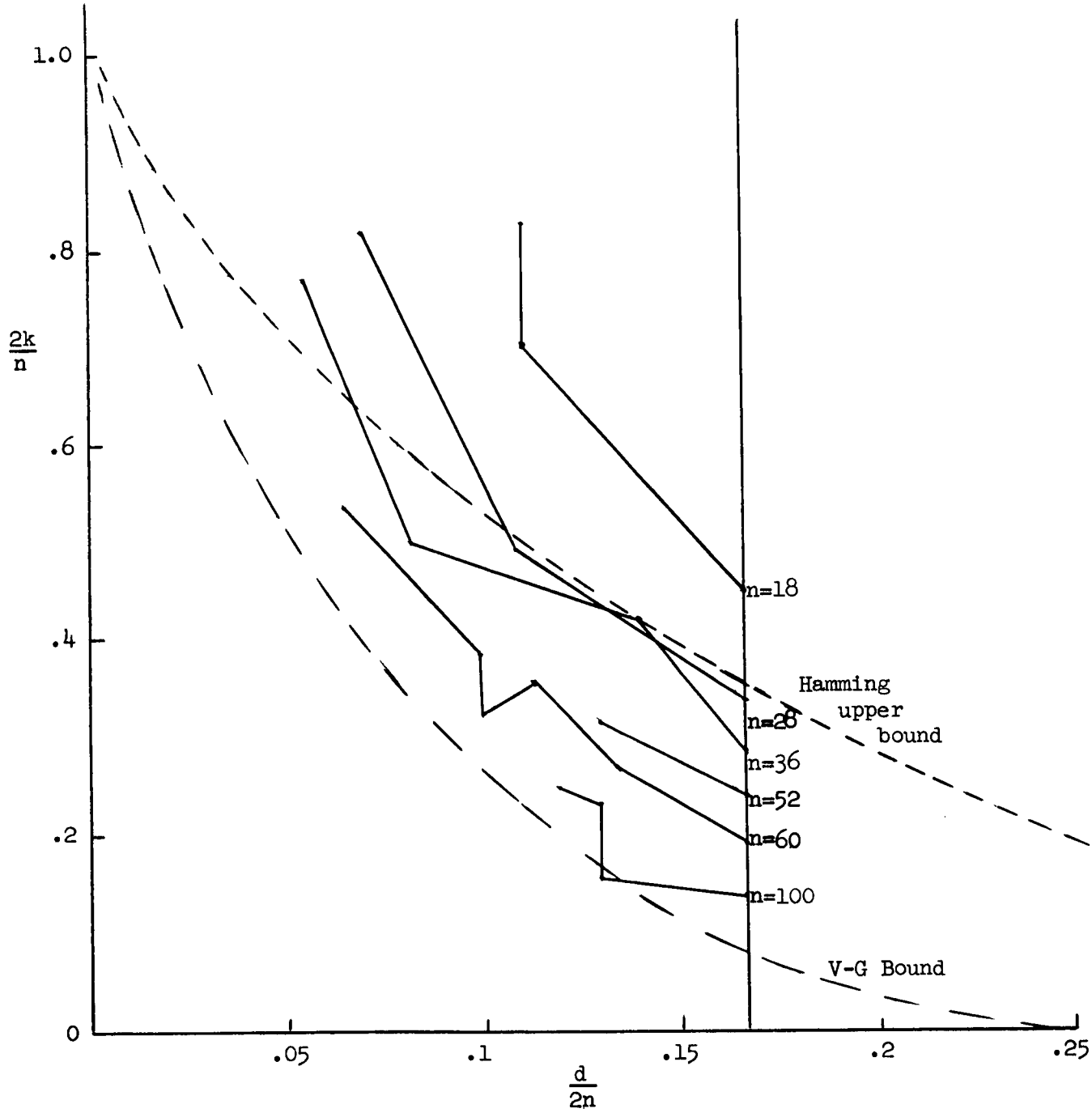


Fig. 1 Transmission Rate ($\frac{2k}{n}$) versus the "Error" Correctability Rate ($\frac{d}{2n}$) for Certain Multiple-Error Correcting Codes of Various Lengths

Before we mention the Fire code analogy in arithmetic codes proposed by Mandelbaum[8], we need some definitions. A number N is said to have length n if $2^n > N > 2^{n-1} - 1$. The power of a number is the largest exponent whose coefficient is non-zero in its binary representation. Finally a number N is said to belong to an exponent e if e is the least positive integer such that p divides $(2^e \pm 1)$.

Here we simply state the theorem which provides the method of constructing the burst error-correcting codes. The proof is contained in the reference[8]. The theorem states that the arithmetic code generated by $A = (2^c-1)p$ will detect any combination of two error bursts $E = 2^iE_1 + 2^jE_2$ provided $c-1 \geq b_1 + b_2$, where b_1, b_2 are the length of the burst errors E_1, E_2 respectively, p is a prime and its power at least as great as the length of the shorter burst, and provided the length of the code is no greater than the least common multiple (LCM) of c and the exponent e to which p belongs. Let $b_2 > b_1$, then $p > 2^{b_1} - 1$. If c is an even integer, then the arithmetic code generated by $A = (2^c-1)p$ can detect any two bursts each of length b or less provided $c \geq 2b$ and $p > 2^b-1$. The length is less or equal to the LCM of c and e, where e is the exponent to which p belongs. This code will correct a burst error of length b or shorter. For a given burst-length b, we limit the choice of p within this bound $2^{b+1} > p > 2^b-1$ for lowest necessary redundancy, since, if $p > 2^{b+1}-1$ we can correct a burst error of longer length. For this choice, p has a length of b+1, and with the minimum choice of c, i.e., $c = 2b$, A has a length of $r = 3b+1$ which is the number of check digits.

Now for any burst error-correcting code of length n, the residues of A belong to mutually exclusive classes. In order to correct burst errors

of length b or less, it is necessary that there must be at least 2^b distinct classes, each containing n distinct residues, i.e.,

$$2^b \leq \frac{A-1}{n} .$$

The arithmetic code generated by $A = (2^c-1)p$, where $2^{b+1} > p > 2^b-1$ and $c = 2b$, corrects burst error of length b. The above inequality is thus satisfied. It follows that

$$2^b < \frac{2^{3b+1}-1}{n} < \frac{2^{3b+1}}{n} ,$$

then

$$n < 2^{2b+1} = 2^{r-b}$$

we have $$r-b - \log_2 n > 0.$$

This is the bound for the ideal case. However, with the arithmetic "Fire" code, a further constraint is given by

$$n \leq \text{LCM}(e,c).$$

Thus for a given b, hence r, we obtain the smallest redundancy by maximizing n. Here we have $c = 2b$ and

$$e = \frac{p-1}{\nu} , \text{ where } \nu \text{ is a positive integer}$$

for $\nu = 1$, e is even and hence $n \leq (p-1) \cdot b$,

$\nu = 2$, if e and c are relative primes, $n \leq (p-1) \cdot b$,

if they are not relative primes, $n < (p-1)\, b$,

$\nu = 3,4,\ldots,$ it is obvious that $n < (p-1) \cdot b$.

Thus a bound for the "Fire" arithmetic code is given by $n < (p-1) \cdot b$

or $$n < (2^{b+1}-1) \cdot b,$$

therefore,

$$r-b-\log_2 n > r-b-\log b - \log(2^{b+1}-1)$$

$$= 2b+1 - \log b - \log(2^{b+1}-1), \text{ as } r = 3b+1.$$

If $\nu = 1$, and p-1 is relative prime to $c = 2b+k$, where $k > 0$, let us investigate whether any improvement in redundancy can be achieved, that is, if there is a greater gain of information bits than that of check bits.

For simplicity, let us write

$$g_o = 2b+1 - \log b - \log(2^{b+1}-1) \text{ for } c = 2b,$$

then

$$g_k = 2b+k+1 - \log(2b+k) - \log(2^{b+1}-1) \text{ for } c = 2b+k.$$

We have an improvement in redundancy, if and only if $g_k < g_o$, i.e., it results in a bound that is closer to zero. For $g_k < g_o$, we must have

$$k - \log(2b+k) < - \log b$$

or simply $$\log \frac{2b+k}{b} > k$$

$$\frac{2b+k}{b} > 2^k$$

or $$k > b(2^k-2),$$

which is only satisfied if $k = 1$. That is, by choosing $c = 2b+1$ such that c and the exponent of $p(= p-1)$ are relative prime to each other, we have gained more than one information bit at the expense of one additional check bit. For $k > 1$, there is no improvement.

Two bounds for c = 2b and c = 2b+1 are shown in Fig. 2, the zero line being the ideal bound. For large b, the two bounds converge. We also show the range of redundancy as decided by the choice of p for each given length of burst-error to be corrected from b = 2 and b = 10. The number of p one can choose increases as b increases. It is noted that the prime p that gives the least redundancy (closest to the bound) is not necessarily the largest prime within the range $2^{b+1} > p > 2^b - 1$. In addition, the primes that result in the least redundancy in the two cases c = 2b and c = 2b+1 are not necessarily the same. We also include the arithmetic codes that are generated by prime numbers as presented by Stein[7] and show that these codes are considerably better than the "Fire" code. In Table III we have an example of the arithmetic Fire Code correcting burst error of length 5 or less to illustrate some of the points mentioned already.

TABLE III

	c = 2b	g_o = 2.68	c = 2b+1	g_1 = 2.55
P	Length n	r-b-log n	Length n	r-b-log n
37	180	3.51	396	3.37
41	20	6.68	220	4.21
43	70	4.87	154	4.73
47	230	3.15	253	4.01
53	260	2.98	572	2.84
59	290	2.82	638	2.68
61	60	5.09	660	2.63

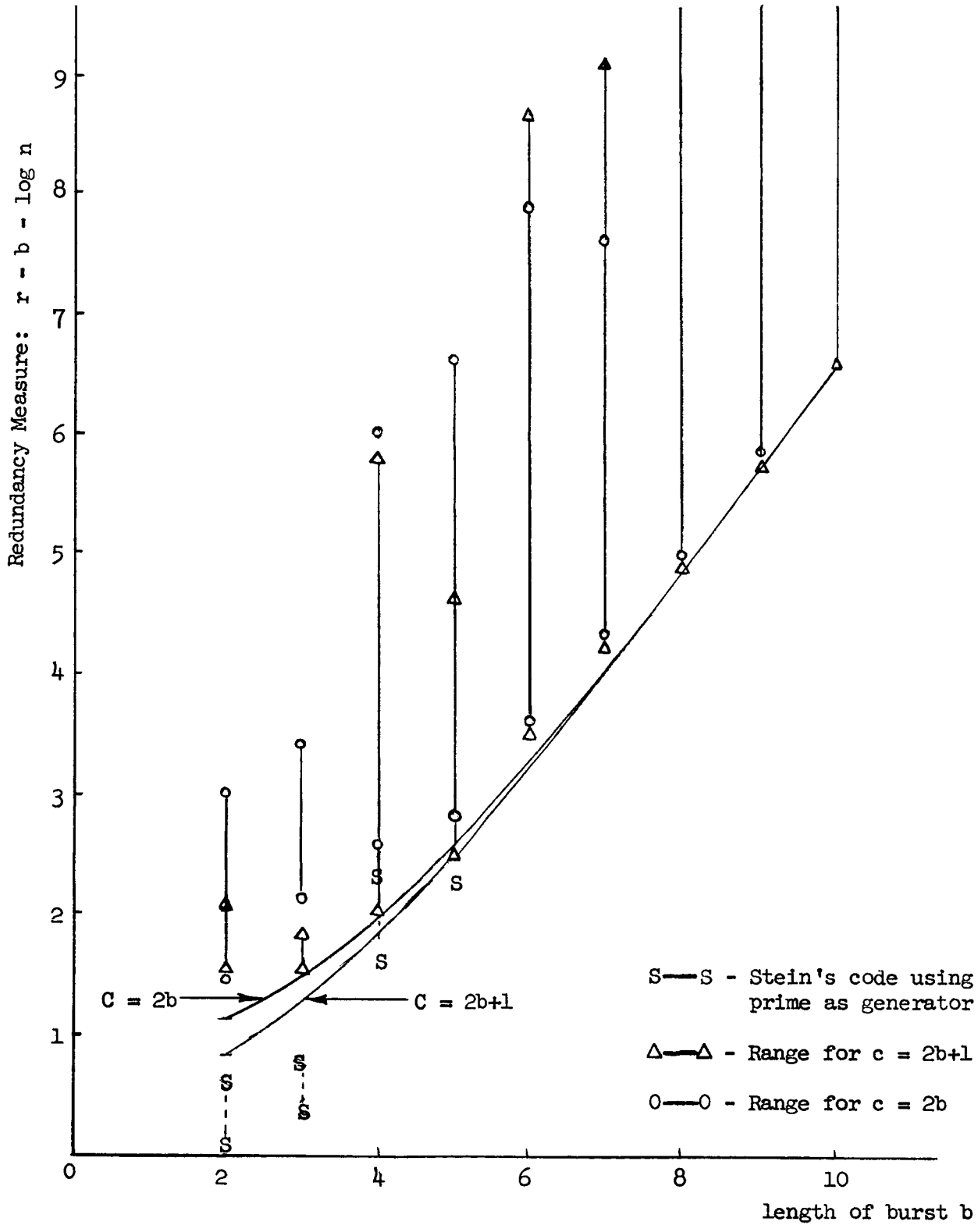


Fig. 2 A Plot of Redundancy Measure vs. Length of Correctable Burst

REFERENCES

1. J. M. Diamond, "Checking Codes for Digital Computers", Proc. IRE, Vol. 43, April 1955.

2. D. T. Brown, "Error Detecting and Correcting Binary Codes for Arithmetic Operations", IRE Transactions Elec. Comp., Vol. EC-9, September 1960.

3. W. W. Peterson, Error-Correcting Codes, The MIT Press and John Wiley & Sons, New York, 1961.

4. D. S. Henderson, "Residue-Class Error Checking Codes", Comm. of ACM, Vol. 4, July 1961.

5. A. J. Bernstein and W. H. Kim, "Linear Codes for Single Error Correction in Symmetric and Assymmetric Computation", IRE Trans., IT-8, January 1962.

6. R. T. Chein, "On Linear Residue Codes for Burst-Error Corrections", IEEE PGIT-10, April 1964.

7. J. J. Stein, "Prime Residue Error-Correcting Codes", IEEE PGIT-10, April 1964.

8. D. Mandelbaum, "Multivalued Arithmetic Burst Error Codes", 1966 IEEE ICR-7, March 1966.

9. John T. Barrows, Jr., "A New Method for Constructing Multiple Error-Correcting Linear Residue Codes", Coordinated Science Laboratory, Report R-277, January 1966.

10. I. M. Vinogradov, Elements of Number Theory, Dover Publications, Inc., 1954.

1. Ivan Niven and Herbert S. Zuckerman, An Introduction to the Theory of Numbers, 2nd edition, John Wiley & Sons, Inc., 1966.

CHAPTER II

NON-BINARY ORTHOGONAL CODES

S. H. Chang

Introduction

An effective set of signals for use in a channel with additive white Gaussian noise is the orthogonal set.[3] Methods of constructing orthogonal continuous waveforms are widely studied. The construction of orthogonal binary waveforms (orthogonal codes) is based primarily on Hadamard matrices. A Hadamard matrix is an orthogonal matrix whose elements are the integers +1 and -1. Hadamard matrices of various orders have been constructed through the generation of pseudo-random sequences of the types (1) maximum length sequences (m-sequences), (2) quadratic residue sequence (or Legendre sequence), (3) twin prime sequence, and (4) Hall sequence.[2] It seems that no such study has been made for the construction of orthogonal matrices using integers (or rational numbers) as elements, although their uses in non-binary coding can be anticipated. Furthermore, it is felt that such study may bring the two areas of endeavor, discrete coding and waveform design, closer to each other.

In the next section the construction of Hadamard matrices by means of binary m-sequences is explained.

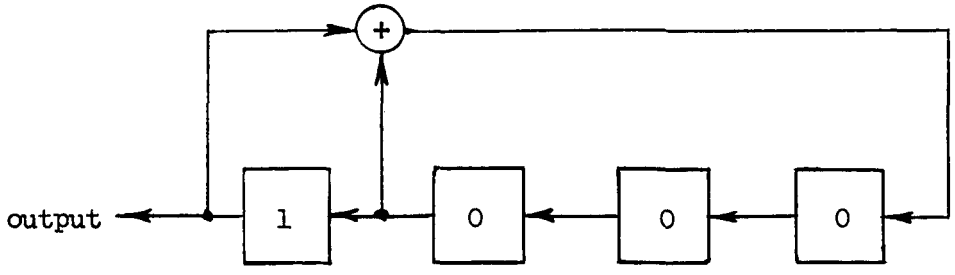
Construction of Hadamard Matrices

It is easier to explain the method of construction by a specific example. Let us choose to construct a 16 × 16 Hadamard matrix. First

we select an irreducible primitive polynomial of degree 4 over GF(2)

$$f(x) = x^4 + x + 1.$$

Then a linear recurrence sequence can be generated by the following shift register circuit when, say, 1000



is originally stored in the register stages before the shifting is started. The sequence of period 15 appears as follows:

1 0 0 0 1 0 0 1 1 0 1 0 1 1 1.

Next, the elements 0,1 of GF(2) are mapped to the two integers, namely,

$$\eta(0) = 1$$
$$\eta(1) = -1.$$

The sequence becomes

-1 1 1 1 -1 1 1 -1 -1 1 -1 1 -1 -1 -1.

This sequence, together with its 14 cyclic shifts form a 15 × 15 matrix. With the final addition of a row and a column of 16 1's each, the construction of Hadamard matrix is completed.

$$H = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\
1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\
1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\
1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\
1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1
\end{bmatrix}$$

This construction procedure is based upon the following property of the m-sequence. Let the infinite sequence be represented by

$$\cdots a_i,\ a_{i+1},\ a_{i+2},\cdots,a_{i+r-1}$$

which is of period $r = 2^m-1$. The autocorrelation function of this sequence relative to the mapping η is

$$\phi(\tau) = \sum_{i=1}^{r} \eta(a_i)\ \eta(a_i-\tau).$$

For the mappings defined above, $\phi(\tau)$ can assume only two values,

$$\phi(\tau) = r \quad \text{if} \quad \tau = 0 \text{ mod. } r$$

$$\phi(\tau) = -1 \quad \text{if} \quad \tau \neq 0 \text{ mod. } r.$$

If we denote the core* of the Hadamard matrix H by H', then

$$(H')(H')^T = (r+1)\ I-J,$$

---

*The core is the matrix before the addition of a row and a column of 1's.

where I is the r × r identity matrix and J is the r × r matrix in which all entries are 1's. Consequently, we have

$$H\,H^T = nI,$$

where n = r + 1. Thus the row vectors of H can be used to design waveforms which are mutually orthogonal. A biorthogonal set of waveforms can be derived if one forms the following matrix:

$$H_b = \begin{bmatrix} H \\ -H \end{bmatrix},$$

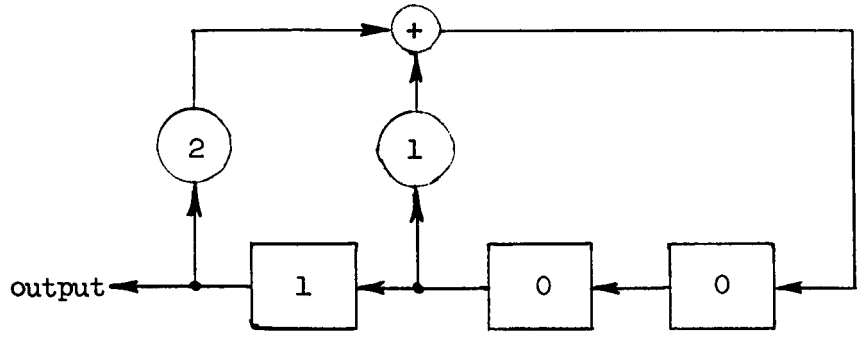
then

$$H_b H_b^T = \begin{bmatrix} nI_{n\times n} & -nI_{n\times n} \\ -nI_{n\times n} & nI_{n\times n} \end{bmatrix}.$$

Orthogonal Matrices Using -1, 0, 1 as Elements

Again we use an example to illustrate the procedure. An m-sequence over GF(3) of period $r = 3^3-1 = 26$ can be generated by using a shift register circuit which corresponds to the irreducible primitive polynomial over GF(3)

$$f(x) = x^3 + 2x + 1.$$



Starting with the stored digits 1 0 0, one period of the m-sequence is as follows:

1 0 0 2 0 2 1 2 2 1 0 2 2 2 0 0 1 0 1 2 1 1 2 0 1 1.

If we use the following mapping of elements GF(3) into elements over rational field

$$\eta(0) = 0$$

$$\eta(1) = 1$$

$$\eta(2) = -1,$$

The sequence becomes

1 0 0 -1 0 -1 1 -1 -1 1 0 -1 -1 -1 0 0 1 0 1 -1 1 1 -1 0 1 1.

In this case, the autocorrelation function has the following values[1]

$$\phi(0) = 2 \cdot 3^{m-1} = \phi(r)$$

$$\phi(\tfrac{r}{2}) = -2 \cdot 3^{m-1}$$

$$\phi(\tau) = 0 \text{ elsewhere in the range } 0 < \tau < r.$$

That is, if one forms a matrix A, with the rows consisting of the above sequence and its r shifts, then

$$AA^T = \begin{bmatrix} \lambda I_{\frac{r}{2} \times \frac{r}{2}} & -\lambda I_{\frac{r}{2} \times \frac{r}{2}} \\ -\lambda I_{\frac{r}{2} \times \frac{r}{2}} & \lambda I_{\frac{r}{2} \times \frac{r}{2}} \end{bmatrix},$$

where $\lambda = 2 \cdot 3^{m-1} = 2 \cdot 3 = 6$, since $m = 2$. The 26 rows can be used in the design of biorthogonal waveforms using -1, 0, 1 as elements. However, the number of waveforms is equal to the dimension of the row vector, instead of twice the dimension as in the case of binary codes.

A simple decomposition of the matrix A enables one to find an orthogonal matrix of the order $\frac{r}{2} \times \frac{r}{2}$. Thus, it is noted that A can be written as

$$A = \begin{bmatrix} B & -B \\ -B & B \end{bmatrix}.$$

And it can be shown that

$$BB^T = \frac{\lambda}{2} I_{\frac{r}{2} \times \frac{r}{2}} .$$

Thus B is indeed such an orthogonal matrix. This matrix is depicted below in its complete form.

$$B = \begin{bmatrix}
1 & 0 & 0 & -1 & 0 & -1 & 1 & -1 & -1 & 1 & 0 & -1 & -1 \\
1 & 1 & 0 & 0 & -1 & 0 & -1 & 1 & -1 & -1 & 1 & 0 & -1 \\
1 & 1 & 1 & 0 & 0 & -1 & 0 & -1 & 1 & -1 & -1 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & -1 & 0 & -1 & 1 & -1 & -1 & 1 \\
-1 & 0 & 1 & 1 & 1 & 0 & 0 & -1 & 0 & -1 & 1 & -1 & -1 \\
1 & -1 & 0 & 1 & 1 & 1 & 0 & 0 & -1 & 0 & -1 & 1 & -1 \\
1 & 1 & -1 & 0 & 1 & 1 & 1 & 0 & 0 & -1 & 0 & -1 & 1 \\
-1 & 1 & 1 & -1 & 0 & 1 & 1 & 1 & 0 & 0 & -1 & 0 & -1 \\
1 & -1 & 1 & 1 & -1 & 0 & 1 & 1 & 1 & 0 & 0 & -1 & 0 \\
0 & 1 & -1 & 1 & 1 & -1 & 0 & 1 & 1 & 1 & 0 & 0 & -1 \\
1 & 0 & 1 & -1 & 1 & 1 & -1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & 0 & 1 & 1 & 1
\end{bmatrix}.$$

The minimum Hamming distance among the row vectors is 9. This is greater than can be provided by Hadamard matrices where the minimum distance is always $\frac{n}{2}$, $n = r+1$. A set of 26 biorthogonal row vectors each of dimension 13 can be obtained by putting a -B matrix under B.

Orthogonal Matrices Using 0, ±1, ±2 as Elements

The m-sequence over GF(5) has its period equal to $r = 5^m-1$. Under similar mappings as before the autocorrelation function $\phi(\tau)$ is again

zero for all values of τ within the period except for $\tau = 0, \frac{r}{2}$. Thus, if

$$\eta(0) = 0$$
$$\eta(1) = 1$$
$$\eta(2) = 2$$
$$\eta(3) = -2$$
$$\eta(4) = -1$$

then

$$\phi(0) = -\phi(\tfrac{r}{2}) = 2 \cdot 5^m$$
$$\phi(\tau) = 0 \quad \text{elsewhere in the range } 0 < \tau < r.$$

Orthogonal Matrices Using 7 Integers as Elements

The autocorrelation function of the m-sequence over GF(7) relative to the mapping

$$\eta(0) = 0$$
$$\eta(1) = 1 \qquad \eta(6) = -1$$
$$\eta(2) = 2 \qquad \eta(5) = -2$$
$$\eta(3) = 3 \qquad \eta(4) = -3$$

behaves differently from those over GF(3) and GF(5) in that it is not zero throughout the ranges $0 < \tau < \frac{r}{2}$, and $\frac{r}{2} < \tau < r$ where $r = p^{m-1} = 7^m - 1$. Rather, it assumes the following values:

$$\phi(0) = 4 \cdot 7^m = \phi(r)$$
$$\phi(t) = \phi(\tfrac{r}{6}) = 2 \cdot 7^m = \phi(5t), \quad t = \frac{r}{p-1} = \frac{r}{6}$$
$$\phi(2t) = \phi(\tfrac{r}{3}) = -2 \cdot 7^m = \phi(4t)$$
$$\phi(3t) = \phi(\tfrac{r}{2}) = -4 \cdot 7^m$$
$$\phi(\tau) = 0 \text{ elsewhere in the ranges } 0 < \tau < \tfrac{r}{2} \text{ and } \tfrac{r}{2} < \tau < r.$$

The values of $\phi(t)$ and $\phi(2t)$ are calculated from the following considerations. There are two primitive elements over GF(7), e = 3 and 5(= -2). Take e = 3 for example, the various powers of 3(mod. 7) are

$$\begin{bmatrix} 3^0 & 3^1 & 3^2 & 3^3 & 3^4 & 3^5 & 3^6 \\ 1 & 3 & 2 & -1 & -3 & -2 & 1 \end{bmatrix}.$$

When $\tau = t$, the autocorrelation function can be expressed[1] as

$$\phi(t) = p^{m-1} \sum_{\substack{\text{all } \alpha \\ \alpha \in GF(7)}} \eta(\alpha)\, \eta(3\alpha)$$

	$\eta(\alpha)$		$\eta(3\alpha)$
	0	×	0
	1	×	3
	2	×	-1
	3	×	2
	-1	×	-3
	-2	×	1
+	-3	×	-2

$$\sum \eta(\alpha)\, \delta(3\alpha) = 2[(1)(3) + (2)(-1) + (3)(2)] = 2(7).$$

When $\tau = 2t$

$$\phi(2t) = p^{m-1} \sum_{\text{all } \alpha} \eta(\alpha)\, \eta(3^2\alpha) = p^{m-1} \sum_{\text{all } \alpha} \eta(\alpha)\, \eta(2\alpha)$$

$$= p^{m-1} \times 2[(1)(2) + (2)(-3) + (3)(-1)] = p^{m-1} \times 2(-7) = -2 \times 7^m.$$

Note that the numbers in the 2 brackets differ by a sign only. If we make a new mapping such as

$$\begin{aligned} 0 &\rightarrow 0 \\ \pm 1 &\rightarrow \pm a \\ \pm 2 &\rightarrow \pm b \\ \pm 3 &\leftrightarrow \pm c, \end{aligned}$$

then it may be possible to equate the value of the number inside the bracket to zeros. That is, we will set

$$(a)(c) + (b)(-a) + (c)(b) = 0.$$

Since there are 3 unknown with one equation, we may assign arbitrary values to two unknown and solve for the third. Thus, let

$$a = 1$$

$$b = 2$$

$$c = \frac{ab}{a+b} = \frac{2}{3}.$$

The new set of elements are in the rational field, namely, 0, ±1, ±2 and $\pm \frac{2}{3}$. If integers are desired, they may be rescaled into the following elements 0, ±3, ±6 and ±2.

As an example, let m = 2, the m-sequence over GF(7) generated by the irreducible primitive polynomial $f(x) = x^2 + 6x + 3$ is of period $p^2-1 = 48$.

1 0 -3 -3 -1 1 -3 1 3 0 -2 -2 -3 3 -2 3 2 0 1 1 -2 2 1 2
-1 0 3 3 1 -1 3 -1 -3 0 2 2 3 -3 2 -3 -2 0 -1 -1 2 -2 -1 -2

The orthogonal matrix of order 24 × 24 using as elements the numbers 0, ±3, ±6, ±2 is shown on the next page.

$$\begin{bmatrix}
3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 & -6 & 2 & 6 & 0 & 3 & 3 & -6 & 6 & 3 & 6 \\
-6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 & -6 & 2 & 6 & 0 & 3 & 3 & -6 & 6 & 3 \\
-3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 & -6 & 2 & 6 & 0 & 3 & 3 & -6 & 6 \\
-6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 & -6 & 2 & 6 & 0 & 3 & 3 & -6 \\
6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 & -6 & 2 & 6 & 0 & 3 & 3 \\
-3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 & -6 & 2 & 6 & 0 & 3 \\
-3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 & -6 & 2 & 6 & 0 \\
0 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 & -6 & 2 & 6 \\
-6 & 0 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 & -6 & 2 \\
-2 & -6 & 0 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 & -6 \\
6 & -2 & -6 & 0 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 & 2 \\
-2 & 6 & -2 & -6 & 0 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 & -2 \\
2 & -2 & 6 & -2 & -6 & 0 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 & -6 \\
6 & 2 & -2 & 6 & -2 & -6 & 0 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 & -6 \\
6 & 6 & 2 & -2 & 6 & -2 & -6 & 0 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 & 0 \\
0 & 6 & 6 & 2 & -2 & 6 & -2 & -6 & 0 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 & 2 \\
-2 & 0 & 6 & 6 & 2 & -2 & 6 & -2 & -6 & 0 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 \\
-3 & -2 & 0 & 6 & 6 & 2 & -2 & 6 & -2 & -6 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 & 3 \\
2 & -3 & -2 & 0 & 6 & 6 & 2 & -2 & 6 & -2 & -6 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 & -2 \\
-3 & 2 & -3 & -2 & 0 & 6 & 6 & 2 & -2 & 6 & -2 & -6 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 & 3 \\
3 & -3 & 2 & -3 & -2 & 0 & 6 & 6 & 2 & -2 & 6 & -2 & -6 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 & -3 \\
2 & 3 & -3 & 2 & -3 & -2 & 0 & 6 & 6 & 2 & -2 & 6 & -2 & -6 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 & -2 \\
2 & 2 & 3 & -3 & 2 & -3 & -2 & 0 & 6 & 6 & 2 & -2 & 6 & -2 & -6 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0 & -2 \\
0 & 2 & 2 & 3 & -3 & 2 & -3 & -2 & 0 & 6 & 6 & 2 & -2 & 6 & -2 & -6 & -3 & -3 & 6 & -6 & -3 & -6 & 3 & 0
\end{bmatrix}$$

Orthogonal Matrices Using 11 Integers as Elements

The factors which contribute to the values of $\phi(\tau)$ of the m-sequence over GF(11) at $\tau = t, 2t, 3t$ and $4t$ are as follows: (note that 2 is a primitive element, its powers are 1, 2, 4, -3, 5, -1, -2, -4, 3, -5, 1).

$$\phi(t): \sum_{\text{all } \alpha} \eta(\alpha)\,\eta(2\alpha) = 2[(1)(2) + (2)(4) + (3)(-5) + (4)(-3) + (5)(-1)] = 2 \times (-22)$$

$$\phi(2t): \sum_{\text{all } \alpha} \eta(\alpha)\,\eta(4\alpha) = 2[(1)(4) + (2)(-3) + (3)(1) + (4)(5) + (5)(-2)] = 2 \times (11).$$

The expressions for $\phi(3t)$ and $\phi(4t)$ contain factors inside brackets same as above. If we make the following mapping

$$0 \rightarrow 0$$
$$\pm 1 \rightarrow \pm a$$
$$\pm 2 \rightarrow \pm b$$
$$\pm 3 \rightarrow \pm c$$
$$\pm 4 \rightarrow \pm d$$
$$\pm 5 \rightarrow \pm e \ ,$$

then equate the expressions for the numbers inside the brackets to be zero,

$$ab + bd + (c)(-e) + (d)(-c) + e(-a) = 0$$

and

$$ad + b(-c) + ca + de + e(-b) = 0.$$

It turns out that if one assigns $a = 1$, $b = 2$, $c = 3$, a solution to the two equations is $d = 4$ and $e = -\frac{1}{2}$. Therefore, a suitable mapping to use for the construction of an orthogonal matrices of 11 integers is such that

$$\eta(0) = 0$$
$$\eta(\pm 1) = \pm 2$$
$$\eta(\pm 2) = \pm 4$$
$$\eta(\pm 3) = \pm 6$$
$$\eta(\pm 4) = \pm 8$$
$$\eta(\pm 5) = \mp 1.$$

Extension of this procedure to $p = 13$ leads to equations whose solutions contain elements of irrational numbers.

Reduction of Types of Elements

Under certain conditions, the number of types of elements can be reduced from a higher prime number to a lower prime number without destroying the orthogonality. For example, the 12 X 12 orthogonal matrix of 5 elements

can be reduced to that of 3 elements by mapping ±2 onto ±1. The resulting matrix is as follows:

$$B = \begin{bmatrix} 1 & 0 & 1 & -1 & 1 & 1 & -1 & 0 & 1 & 1 & 1 & 1 \\ -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & 0 & 1 & 1 & 1 \\ -1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & 0 & 1 & 1 \\ -1 & -1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & 0 & 1 \\ -1 & -1 & -1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & 0 \\ 0 & -1 & -1 & -1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 \\ 1 & 0 & -1 & -1 & -1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 \\ -1 & 1 & 0 & -1 & -1 & -1 & -1 & 1 & 0 & 1 & -1 & 1 \\ -1 & -1 & 1 & 0 & -1 & -1 & -1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & -1 & -1 & -1 & -1 & 1 & 0 & 1 \\ -1 & 1 & -1 & -1 & 1 & 0 & -1 & -1 & -1 & -1 & 1 & 0 \\ 0 & -1 & 1 & -1 & -1 & 1 & 0 & -1 & -1 & -1 & -1 & 1 \end{bmatrix}.$$

Other examples are listed in the following table:

Original Number of Elements	Reduced Number of Elements	Mapping of Elements
5	3	a = b = 1
7	5	a = b = 2, c = 1
7	3	a = 1, b = c = 0
11	9	a = 2, b = c = 6, d = 10, e = 1
11	7	a = 3, b = c = d = 6, e = 2
11	3	a = b = c = d = 0, e (any values)

Products of Orthogonal Matrices

There are two types of products of orthogonal matrices which lead to new orthogonal matrices. One is the ordinary product and the other is the Kronecker or tensor product. This statement is true because, assuming A and B are orthogonal matrices

(1) $AA^T = \lambda_a I$ and $BB^T = \lambda_b I$

$$(AB) \cdot (AB)^T = A(BB^T)\, A^T = A(\lambda_b I)\, A^T = \lambda_a \lambda_b I$$

(A and B of the same rank);

$$(2)\quad (A \times B) \cdot (A \times B)^T = (A \times B) \cdot (A^T \times B^T) = (AA^T) \times (BB^T)$$

$$= (\lambda_a I_a) \times (\lambda_b I_b) = \lambda_a \lambda_b I_{ab} \cdot$$

Note that A and B are not necessarily of the same rank.

Some examples for each of the two types of products is given below.

(1)

$$A \cdot B = \begin{bmatrix} 0 & 1 & -1 & -1 \\ 1 & 0 & 1 & -1 \\ 1 & 1 & 0 & 1 \\ -1 & 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & -1 & -1 \\ 1 & 0 & 1 & -1 \\ 1 & 1 & 0 & 1 \\ -1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -2 & 0 & -2 \\ 2 & 1 & -2 & 0 \\ 0 & 2 & 1 & -2 \\ 2 & 0 & 2 & 1 \end{bmatrix}$$

(3 elements) (3 elements) (5 elements)

$$A \cdot B = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 2 & 1 & 2 \\ 2 & 0 & 2 & -1 \\ 1 & -2 & 0 & 2 \\ 2 & 1 & -2 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 3 & 1 & 1 \\ 3 & -5 & -1 & 1 \\ 1 & 1 & -5 & -3 \\ 1 & -1 & 3 & -5 \end{bmatrix} \cdot$$

(2 elements) (5 elements) (6 elements)

(2)

$$A \times B = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & -1 & -1 \\ 1 & 0 & 1 & -1 \\ 1 & 1 & 0 & 1 \\ -1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & -1 & -1 & 0 & 1 & -1 & -1 \\ 1 & 0 & 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ -1 & 1 & 1 & 0 & -1 & 1 & 1 & 0 \\ 0 & 1 & -1 & -1 & 0 & -1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 0 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 & 0 & -1 \\ -1 & 1 & 1 & 0 & 1 & -1 & -1 & 0 \end{bmatrix} .$$

(2 × 2) (4 × 4) (8 × 8)

It is evident that these two types of products provide recursive methods for generating new orthogonal matrices from old ones.

Construction by Inspection

The following orthogonal matrices are obtained by inspection

(1) 2×2 (3 level or less)

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

(2) 4×4 (7 level or less)

$$\begin{bmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{bmatrix}$$

(3) 8×8 (15 level or less)

$$\begin{bmatrix} a & b & -c & d & e & f & g & h \\ -b & a & d & c & -f & e & -h & g \\ c & d & a & b & -g & h & e & -f \\ -d & -c & -b & a & -h & -g & f & e \\ -e & f & g & h & a & -b & c & -d \\ -f & -e & -h & g & b & a & -d & -c \\ -g & h & -e & -f & -c & d & a & -b \\ -h & -g & f & -e & d & c & b & a \end{bmatrix}.$$

By assigning suitable values to the letters, some of which may have the same value, orthogonal matrices of various elements can be constructed.

Summary and Discussions

The purpose of this study is to explore the use of the m-sequence for the construction of orthogonal matrices using more than two elements 1 and -1. It is based upon the properties of the autocorrelation function $\phi(\tau)$ of the m-sequences of p elements ($p = 3, 5, 7, 11$) relative to certain mapping η. The autocorrelation function has the same period as the m-sequence, i.e., $r = p^m - 1$. Under symmetrical mapping, its values at $\tau = 0$ and $\tau = \frac{r}{2}$ differ in sign, but equal in magnitude. Therefore, unlike the case for $p = 2$, a segment equal to half period of the sequence is used for the construction of the orthogonal matrices. Furthermore, for cases $p = 7$ and 11, $\phi(\tau)$ assumes non-zero values under ordinary mapping for τ

smaller than a half period. These are restored to zero by suitable remapping. Similar procedures applied to the cases for $p > 11$ result in solutions in the elements of irrational or complex field.

It is possible to derive orthogonal matrices using smaller number of elements from those using larger number of elements. It is also possible to obtain matrices using larger number of elements from the products (ordinary) of matrices using smaller number of elements. Kronecker products provide a method of expanding the sizes of orthogonal matrices.

The design of orthogonal matrices using more than two elements is an attempt to use multi-level digits in the design of waveforms for coding. Such waveforms may match with the existing channels better than those using two levels only. It shoudl also be noted that the minimum Hamming distance (or other measure of distance) among the row vectors of the orthogonal matrix is usually larger than $\frac{n}{2}$ which is a fixed value for any $n \times n$ Hadamard matrix using 2 elements.

REFERENCES

1. N. Zierler, "Linear Recurring Sequences", J. Soc. Indust. Appl. Math., 7,31-48, 1959, also in W. H. Kautz (editor), Linear Sequential Switching Circuits, Holden-Day, 1965.

2. E. F. Beckenbach (editor), Applied Combinatorial Mathematics, Chapter 13, "Block Designs", by M. Hall, Jr., John Wiley & Sons, 1964.

3. S. W. Golomb (editor), Digital Communications with Space Applications, Chapter 4, "Codes with Special Correlation", by L. D. Baumert, Prentice-Hall, 1964.

CHAPTER III

ERROR-COUNTING SCHEMES

L. J. Weng

Introduction

Recently, many block codes have been constructed to cope with random errors. The error-correcting code is designed to correct t_c or less erroneous digits in each code block of length n. The error-detecting code is used to determine whether or not a code block of length n contains errors (assuming that there are no more than t_d corrupted digits in each code block). Unfortunately, the decoding scheme for the error-correcting codes is, in general, rather complex, and the error detecting code reveals no information about how badly a code block is corrupted. Therefore, it is desirable to have an intermediate code which can be decoded rather simply in comparison to the error-correcting code while giving more information than the error-detecting code.

The concept of error-counting is developed to satisfy this requirement. The decoding procedure of such a code gives the number of erroneous digits without referring to their exact positions. In order to be competitive, it is required that the decoding procedure be far less complicated than that of an error-correcting code.

There are two ways to obtain error-counting schemes, namely, the constructing of new codes and the use of inherent error-counting property of existing error-correcting codes. Some results along both lines will be given.

The Construction of Error-Counting Codes

The technique of block design* has been incorporated here to find a suitable parity-check matrix. Examples of two classes of error-counting codes so constructed are given below:

(a) n-error-counting codes derived from permuting n × n identity matrix. The parity-check matrix is given by

$$\left[\begin{array}{cccccccc}
P & I_n & I_n & I_n & I_n & \cdots & I_n & I_n & I_n \\
\hline
P\pi & I_n & I_n\pi & I_n\pi^2 & I_n\pi^3 & \cdots & I_n\pi^{n-3} & I_n\pi^{n-2} & I_n\pi^{n-1} \\
\hline
P\pi^2 & I_n & I_n\pi^2 & I_n\pi^3 & I_n\pi^4 & \cdots & I_n\pi^{n-2} & I_n\pi^{n-1} & I_n\pi \\
\hline
\vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
\hline
P\pi^{n-2} & I_n & I_n\pi^{n-2} & I_n\pi^{n-1} & I_n\pi & \cdots & I_n\pi^{n-5} & I_n\pi^{n-4} & I_n\pi^{n-3} \\
\hline
P\pi^{n-1} & I_n & I_n\pi^{n-1} & I_n\pi & I_n\pi^2 & \cdots & I_n\pi^{n-4} & I_n\pi^{n-3} & I_n\pi^{n-2}
\end{array}\right],$$

where

(1) P is an n × n matrix whose entries are all zero except the first column which contains all 1's;

(2) π is a cyclic permutation matrix (to the right) for postmultiplication;

and (c) I_n is an n × n identity matrix.

---

*Edwin F. Beckenbach (editor), Applied Combinatorial Mathematics, Chapter 13, John Wiley & Sons, 1964.

The syndrome $\underline{s}$ of a received vector (or sequence) $\underline{r}$ is calculated by

$$\underline{s} = \underline{r} H^T . \tag{1}$$

It can be shown that the syndrome is classified according to its pattern and distribution of weights. This classification corresponds to the different number of errors in a received sequence.

For example, the parity-check matrix of a (12,3) 3-error-counting code is

$$H = \begin{bmatrix} 100 & 100 & 100 & 100 \\ 100 & 010 & 010 & 010 \\ 100 & 001 & 001 & 001 \\ \\ 010 & 100 & 001 & 010 \\ 010 & 010 & 100 & 001 \\ 010 & 001 & 010 & 100 \\ \\ 001 & 100 & 010 & 001 \\ 001 & 010 & 001 & 100 \\ 001 & 001 & 100 & 010 \end{bmatrix} .$$

The syndrome classification is as follows:

(1) $W[\underline{s}] = 0$ which implies no error, where $W[\underline{s}]$ denotes the weight of the syndrome $\underline{s}$.

(2) $W[\underline{s}] = 3$, which is further classified as follows.

(a) Let the syndrome $\underline{s}$ be divided into three sub-syndromes $\underline{s_1}$, $\underline{s_2}$, $\underline{s_3}$, each containing 3 digits, i.e.,

$$\underline{s} = \underline{s_1 \; s_2 \; s_3} .$$

If $W[\underline{s_1}] = W[\underline{s_2}] = W[\underline{s_3}] = 1$ or if one of the sub-syndromes is of weight 3 and the other two of weight zero, then the received block contains a single error.

(b) Otherwise there are 3 or more errors.

(3) $W[\underline{s}]$ = 2, 4 or 6 (even) which implies 2 errors.

(4) $W[\underline{s}]$ = odd number > 3 which implies 3 or more errors.

Although the objectives of this class of codes are achieved by simple classifications of the syndromes, it is a class of high-redundancy. Furthermore, for each pre-specified error-countability requirement only one code can be obtained. In the following, we attempt to construct some more efficient codes by using "doubly cyclic codes". By doubly cyclic code we mean that if $\underline{v} = \underline{v_1}\ \underline{v_2}$ is a code word, then $\underline{v_1'}\ \underline{v_2'}$ is also a code word where $\underline{v_1'} = \underline{v_1}\pi$ and $\underline{v_2'} = \underline{v_2}\pi$ and π is a cyclic permutation matrix. Note that $\underline{v_1}\ \underline{v_2'}$ is not necessarily a code word. An example of 3-error-counting (20,10) code is given below:

$$H = \begin{bmatrix}
1&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&1&0&0&1\\
1&1&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&1&0&0\\
0&1&1&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&1&0\\
1&0&1&1&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&1\\
0&1&0&1&1&0&0&0&0&0&1&0&0&1&1&0&0&0&0&0\\
0&0&1&0&1&1&0&0&0&0&0&1&0&0&1&1&0&0&0&0\\
0&0&0&1&0&1&1&0&0&0&0&0&1&0&0&1&1&0&0&0\\
0&0&0&0&1&0&1&1&0&0&0&0&0&1&0&0&1&1&0&0\\
0&0&0&0&0&1&0&1&1&0&0&0&0&0&1&0&0&1&1&0\\
0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&1&0&0&1&1
\end{bmatrix}.$$

The syndrome patterns and weights can be classified according to the following:

(1) $W[\underline{s}] = 0$ which implies no error.

(2) $W[\underline{s}] = 3$ which is further classified as follows:

(a) If $\underline{s}$ is a shifted version of either

1 1 0 1 0 0 0 0 0 0

or

1 1 0 0 1 0 0 0 0 0 ,

then the received sequence contains only a single error.

(b) Otherwise, there are 3 or more errors.

(3) $W[\underline{s}]$ = even integer which implies two errors.

(4) $W[\underline{s}]$ = odd integer > 3 which implies 3 or more errors.

Error-Counting Property of B-C-H Codes

A sub-class of B-C-H codes can be used as error-counting codes by simplifying the step-by-step decoding procedure suggested by Massey.[1]

For a t-error-correcting binary B-C-H code, the matrix

$$L_t = \begin{bmatrix} s_1 & 1 & 0 & 0 & \cdots & 0 \\ s_3 & s_2 & s_1 & 1 & \cdots & 0 \\ \cdot & & & & & \\ \cdot & & & & & \\ \cdot & & & & & \\ s_{2t-1} & s_{2t-2} & s_{2t-3} & s_{2t-4} & \cdots & s_t \end{bmatrix}$$

is singular if the weight of the error pattern is t-1 or less, and is non-singular if the weight of the error pattern is t or t+1. s_i's, the power sums of the errors, are elements of $GF(2^m)$. A partial list

of a subclass of the B-C-H code given in Table I shows that L_{t-1} the matrix can be obtained by deleting the last row and the last column of the matrix L_t. Similarily L_{t-2} can be obtained from L_{t-1} and so on until L_1 is obtained. Each of the L_i's has the property that it is singular if the weight of the error pattern is i-1 or less and is non-singular if the weight of the error pattern is i or i+1. The error-counting procedures are as follows:

Step 0 - set $i = t$,

Step 1 - calculate det L_i,

Step 2 - if det $L_i \neq 0$, go to Step 4; otherwise go to Step 3,

Step 3 - decrease i by 1 and go to Step 1,

Step 4 - number of errors = i,

Step 5 - stop.

This is an easy error-counting procedure provided a calculator over $GF(2^m)$ is available. The calculation over $GF(2^m)$ is, in general, far more complicated than that over GF(2).[2] In order to simplify such calculations which are used in Step 1, we establish the following notations and theorem that facilitates the determination of the value of det L_i.

Table I A Partial List of B-C-H Codes Adaptable to Error-Counting

n	k	t	n	k	t
7	4	1	127	120	1
15	11	1		113	2
	7	2		106	3
	5	3		99	4
31	26	1		92	5
	21	2		85	6
	16	3		78	7
			255	247	1
63	57	1		239	2
	51	2		231	3
	45	3		223	4
	39	4		215	5
	36	5		207	6
	30	6		199	7
				191	8
				187	9
				179	10
				171	11
				163	12
				155	13
				147	14
				139	15

Let 0, α^0, α^1,...,α^{2^m-1} be elements of GF(2^m). If each α^i is mapped into a column vector $\alpha^i]$ of m elements over GF(2), then $\alpha^i]$ can be obtained by

$$\alpha^i] = T_0^i \alpha^0] = T_0^i \begin{bmatrix} 1 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix},$$

where T_o is the companion matrix as defined by

$$T_o = \left[\alpha^1] \ \ldots \ \alpha^m]\right]$$

$$= \begin{bmatrix} 0 & 0 & & 0 & \\ 1 & 0 & & 0 & \\ \cdot & \cdot & \cdots & \cdot & \alpha^m] \\ \cdot & \cdot & & \cdot & \\ \cdot & \cdot & & \cdot & \\ 0 & 0 & & 1 & \\ 0 & 0 & & 0 & \end{bmatrix}.$$

For each L_j, with elements written in terms of α^i's we have

$$L_j = \begin{bmatrix} a_{11}\alpha^{i_{11}} & a_{12}\alpha^{i_{12}} & \ldots & a_{1j}\alpha^{i_{1j}} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{j1}\alpha^{i_{j1}} & a_{j2}\alpha^{i_{j2}} & \ldots & a_{jj}\alpha^{i_{jj}} \end{bmatrix},$$

where a_{kh}'s are either one or zero. We can form a binary matrix

$$L_j' = \begin{bmatrix} a_{11}T_o^{i_{11}} & a_{12}T_o^{i_{12}} & \ldots & a_{1j}T_o^{i_{1j}} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{j1}T_o^{i_{j1}} & a_{j2}T_o^{i_{j2}} & \ldots & a_{jj}T_o^{i_{jj}} \end{bmatrix}.$$

The matrix L_j is a $j \times j$ matrix over $GF(2^m)$ and the matrix L_j' is a $jm \times jm$ matrix over $GF(2)$.

Now the following theorem can be established:

<u>Theorem</u>

$\det L_j = 0$ if and only if $\det L_j' = 0$.

Proof

If det $L_j = 0$, then there exists at least a set of columns (or rows) which are linearly dependent.

Let

$$\alpha^{s_1}\begin{bmatrix} a_{1k_1}\alpha^{i_1k_1} \\ \vdots \\ a_{jk_1}\alpha^{i_jk_1} \end{bmatrix} + \ldots + \alpha^{s_r}\begin{bmatrix} a_{1k_r}\alpha^{i_1k_r} \\ \vdots \\ a_{jk_r}\alpha^{i_jk_r} \end{bmatrix} = 0 \qquad (1)$$

or

$$\begin{bmatrix} a_{1k}\,\alpha^{i_1k+s_1} \\ \vdots \\ a_{jk}\,\alpha^{i_jk+s_1} \end{bmatrix} + \ldots + \begin{bmatrix} a_{1k_r}\alpha^{i_1k_r+s_r} \\ \vdots \\ a_{jk_r}\alpha^{i_1k_r+s_r} \end{bmatrix} = 0 \qquad (2)$$

$$r < j$$

$$a_{\ell k}\alpha^{i_\ell k+s_1} + \ldots + a_{\ell k_1}\alpha^{i_jk+s_r} = 0 \text{ for } \ell = 1,\ldots,j. \qquad (3)$$

This implies that

$$\left[a_{\ell k}T_o^{i_\ell k+s_1} + \ldots + a_{\ell k_r}T_o^{i_1k+s_r}\right]\alpha^f = 0 \text{ for } \ell = 1,\ldots,j \quad f = 1,2,3,\ldots,m-1. \qquad (4)$$

$$a_{\ell k}T_o^{i_\ell k+s_1} + \ldots + a_{\ell k}T_o^{i_1k+s_r} = 0 \text{ for } \ell = 1,\ldots,j. \qquad (5)$$

Now suppose that

$$\det L_j \neq 0 \quad \text{and} \quad \det L_j' = 0.$$

$\det L_j \neq 0$ implies that Equations (1), (2) and (3) do not hold.

But $L_j' = 0$ implies that a set of columns are linearly dependent. Suppose this set of columns are chosen such that $d_k (d_k \leq m)$ columns are from

$$\begin{bmatrix} a_{1k} T_o^{i_{1k}} \\ \vdots \\ a_{jk} T_o^{i_{jk}} \end{bmatrix}. \tag{6}$$

But $a_{1k} T_o^{i_{1k}} = a_{1k} \left[\alpha^{i_{1k}} \; a^{i_{1k}} \right] \ldots a^{i_{1k+m-1}} \Big] \Big]$, hence a linear combination d_k columns of which is

$$a_{1k} \left[\left(\alpha^{j_1} + \alpha^{j_2} \ldots + \alpha^{j_{dk}} \right) \alpha^{i_{1k}} \right]$$

or

$$a_{1k} \left[\beta^k \, \alpha^{i_{1k}} \right]. \tag{7}$$

Therefore, the d_k column combination of (6) is

$$\begin{bmatrix} a_{1k} \, \beta^k \, \alpha^{i_{1k}} \\ a_{2k} \, \beta^k \, \alpha^{i_{2k}} \\ \vdots \\ a_{jk} \, \beta^k \, \alpha^{i_{jk}} \end{bmatrix}. \tag{8}$$

Then the linear combination of columns can be written as

$$\sum_{k=1}^{\ell} \begin{bmatrix} a_{1k}\,\beta^k\,\alpha^{i_{1k}} \\ a_{2k}\,\beta^k\,\alpha^{i_{2k}} \\ \vdots \\ a_{jk}\,\beta^k\,\alpha^{i_{jk}} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{9}$$

or equivalently

$$\sum_{k=1}^{\ell} a_{hk}\,\beta^k\,\alpha^{i_{hk}} = 0 \quad \text{for} \quad h = 1,2,\ldots,j. \tag{10}$$

Returning to $GF(2^m)$ field, we have

$$\sum_{k=1}^{\ell} a_{hk}\,\beta^k\,\alpha^{i_{hk}} = 0, \quad h = 1,2,\ldots,j, \tag{11}$$

where β^k's are elements of $GF(2^m)$. Therefore, we can obtain ℓ columns of L_j such that they are linearly dependent. This is in contradiction to our previous assumption. Q.E.D.

With the help of this theorem, the error-counting process can be greatly simplified. In Step 1 we need only to calculate det L_i' which is a binary matrix instead of det L_i which is a matrix over $GF(2^m)$. Furthermore, all the elements of det L_i' can be obtained from error syndromes and a linear shift-register.

References

1. J. L. Massey, "Step-by Step Decoding of the Bose-Chaudhuri-Hocquenghem Codes", IEEE Transactions on Information Theory, Vol. IT-11, October 1965, pp. 580-585.

2. T. C. Bartee and D. I. Schneider, "Computation with Finite Fields", Information and Control, 1963, pp. 79-98.

3. W. W. Peterson, Error-Correcting Codes, MIT - Wiley, 1961.

CHAPTER IV

DATA TRANSMISSION BY PULSE AMPLITUDE MODULATION THROUGH A NOISY CHANNEL WHICH HAS BEEN RANDOMLY SELECTED*

R. A. Gonsalves

Introduction

We consider here a design of a fixed equalizer for Pulse Amplitude Modulation (PAM) signals transmitted over a noisy, randomly-selected channel. The linear, time-invariant equalizer is chosen to minimize the mean-square error between transmitted and received message sequences when averaged over all realizations of the channel, the additive noise sequence, and the message sequence.

By "randomly-selected" we mean that the channel, assumed linear and time-invariant, has a system function $R(f)$ which is a realization of a stochastic process. One of the results of the analysis is to determine what characteristics of this process must be known in order to design the fixed equalizer using our mean-square error criterion. As one would anticipate, only certain second order statistics are required.

Although we assume that the channel is time-invariant, the results may be applicable to the equalization of a time-varying channel when the variations are slow relative to the correlation times of equalizer output signal and noise. In fact, the fixed equalizer might be used to best advantage in

---

*This work was done in collaboration with D. W. Tufts of Harvard University, and is a continuation of studies initiated at Bell Telephone Laboratories, North Andover, Massachusetts.

conjunction with a variable, automatic equalizer[1,2] for a slowly time-varying channel. That is, due to the randomness in the system the automatic equalizer will be matched to the channel only in a probabilistic sense, although the residual errors may be small. To minimize the effects of mismatch one would follow the adjustable equalizer by the fixed equalizer considered here. For such a system this analysis may be used to generate appropriate specifications on the automatic equalizer.

The design of linear, time-invariant equalizers for a noisy, fixed channel has been treated in detail (see references 3-6 and 9-13 for examples). The analysis of a noiseless, single-side-band system with small sampling time error and carrier phase error has been performed by Franks.[7] The noisy channel with timing jitter has also been studied.[5,8] These analyses are special cases of the more general problem treated here, except that joint transmitter-received optimization is treated in reference [3], [5], [6] and [8] and finite message sequences are assumed in reference [2].

The System Model

The model we will study is shown in Fig. 1. In that figure the received PAM signal before noise addition is $y(t)$, a real waveform given by

$$y(t) = \sum_{k=-\infty}^{\infty} a_k \, r(t-kT), \tag{1}$$

where $r(t)$ is the received pulse shape with Fourier transform $R(f)$,

$$R(f) \equiv \int_{-\infty}^{\infty} r(t) \, e^{-j2\pi ft} \, dt. \tag{2}$$

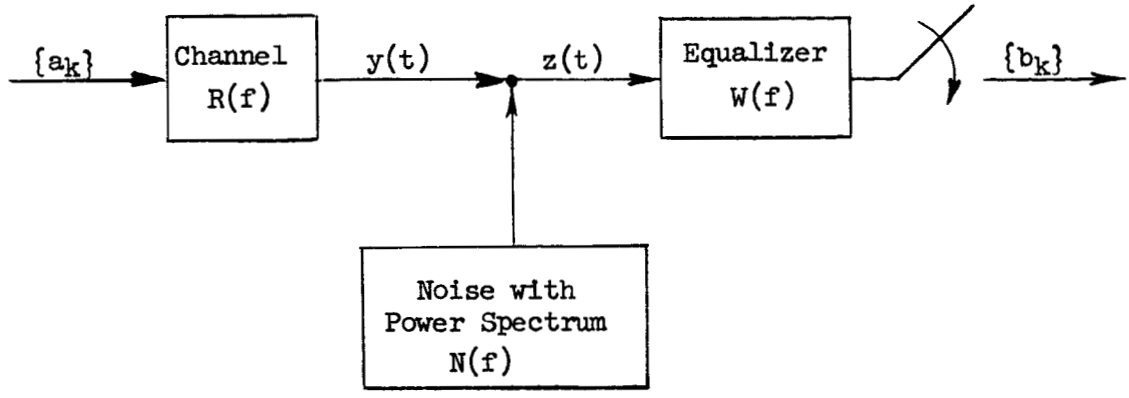


Fig. 1

The random message sequence $\{a_k\}$ is assumed to be stationary with message spectrum M(f), a periodic spectral density function given by the formula

$$M(f) = m_0 + 2\sum_{i=1}^{\infty} m_i \cos 2\pi iTf \qquad (3)$$

in which $\{m_i\}$ is the discrete autocorrelation function of the random sequence $\{a_k\}$. The additive noise is assumed to be stationary with known power spectrum N(f). W(f), the filter to be determined, has a real impulse response which will, in general, be non-zero for $t < 0$. The sampler samples the output of W(f) at kT seconds (plus a fixed T' seconds to allow approximation of the non-realizable W(f)) to give the received sequence $\{b_k\}$.

The Fixed Equalizer

Defining I_R as the mean-square error between a_k and b_k when averaged over all possible message sequences and noise sequences, one can show that I_R is given by the formula [5] [6]

$$I_R = m_0 - \int_{-\infty}^{\infty} M(f)\, R^*(f)\, W^*(f) \left[2 - \frac{1}{T}\sum_{i=-\infty}^{\infty} R\left(f - \frac{i}{T}\right)\right] df + \int_{-\infty}^{\infty} N(f)\,|W(f)|^2\, df, \qquad (4)$$

which is independent of the time index of k because of the assumed stationarity of message and noise. In (4) and throughout an asterisk denotes complex conjugation. Averaging I_R over all realizations of R(f), we have the average error A,

$$A \equiv \overline{I}_R \ , \tag{5}$$

which is to be minimized by proper choice of W(f).

A straightforward application of the calculus of variations yields the following condition on W(f) for A to be a minimum:

$$\frac{N(f)}{M(f)} W(f) + \frac{1}{T} \sum_{k=-\infty}^{\infty} \overline{R^*(f)\, R(f - \tfrac{k}{T})}\, W(f - \tfrac{k}{T}) = \overline{R^*(f)} \tag{6}$$

for all frequencies except those at which all R(f)'s are zero, and W(f) = 0 elsewhere. For such a W(f) the resulting A_{min} is

$$A_{min} = m_0 - \int_{-\infty}^{\infty} M(f)\, W(f)\, \overline{R(f)}\, df. \tag{7}$$

We will discuss the solution of (6) for W(f) momentarily, but first we notice that for solution we must know the average channel transmission $\overline{R(f)}$, which is the mean of the process and $\overline{R^*(f)\, R(f - \frac{k}{T})}$, the frequency autocorrelation of the process, at integer multiples of the frequency shift $\frac{1}{T}$ cps. These are the quantities which must be determine experimentally or which must be modelled to find the optimum equalizer.

Following Reference [8], we solve for W(f) by writing (6) for a set of frequencies $u + \frac{i}{T}$, $i = 0, \pm 1, \pm 2, \ldots$, where u lies in the interval $(0, \frac{1}{T})$. In certain cases the resulting doubly infinite set of equations (one for each i) can be solved using the theory of Toeplitz matrices. Note that we need W(f) only for $f \geq 0$ since, for the real time functions considered here, $W(-f) = W^*(f)$.

In cases for which the channel is known to be bandlimited the solution can be quite simple. For example, suppose

$$R(f) = 0 \quad \text{for } |f| \geq \frac{1}{2T} . \tag{8}$$

(The pulse rate of $\frac{1}{T}$ pulses per second then correspnds to the Nyquist rate.) Examination of (6) reveals that $W(f)$ must be zero for $f \geq \frac{1}{2T}$ and for $f < \frac{1}{2T}$, $W(f)$ becomes

$$W(f) = \frac{\overline{R^*(f)}}{\frac{N(f)}{M(f)} + \frac{1}{T}\overline{|R(f)|^2}} . \tag{9}$$

From (9) we see that if the left-hand denominator term dominates the right-hand term, the low signal-to-noise-ratio case, $W(f)$ reduces to a filter matched to the average transmission characteristic $\overline{R(f)}$. In the high signal-to-noise-ratio case the filter $W(f)$ attenuates those spectral portions for which $\overline{|R(f)|^2}$ is large, reflecting the large expected variations in channel transmission at those frequencies; also, if $R(f)$ is nearly constant, $W(f) \approx \frac{T}{R(f)}$, as should be expected.

Now suppose that

$$R(f) = 0 \quad \text{for } |f| > \frac{1+\lambda}{2T} , \tag{10}$$

and

$$0 < \lambda < 1. \tag{11}$$

λ is a measure of the "excess bandwidth"; that is, we are pulsing at rate $\frac{1}{T}$, slower than the Nyquist rate of $\frac{1+\lambda}{T}$. Then examination of (6) reveals that $W(f)$ must be zero for $f > \frac{1+\lambda}{2T}$, and for $0 \leq f \leq \frac{1-\lambda}{2T}$, Equation (9)

must still hold. However, for $\frac{1-\lambda}{2T} < f < \frac{1+\lambda}{2T}$, we follow the procedure described above to show that W(f) must satisfy the matrix equation

$$\begin{bmatrix} E_1 & \frac{1}{T}\overline{R_1^* R_2} \\ \frac{1}{T}\overline{R_2^* R_1} & E_2 \end{bmatrix} \begin{bmatrix} W_1 \\ W_2 \end{bmatrix} = \begin{bmatrix} \overline{R_1^*} \\ \overline{R_2^*} \end{bmatrix}, \tag{12}$$

where W_1 denotes W(f), W_2 denotes $W(f - \frac{1}{T})$, etc., and

$$E(f) \equiv \frac{N(f)}{M(f)} + \frac{1}{T}\overline{|R(f)|^2} . \tag{13}$$

Solving (12) for W(f) we have

$$W_1 = \frac{\overline{R_1^* E_2} \quad \frac{1}{T}\overline{R_2^*}\ \overline{R_1^* R_2}}{E_1 E_2 - (\frac{1}{T})^2 \overline{|R_1^* R_2|^2}} . \tag{14}$$

To be more specific in the preceding example assume that the randomness in R(f) resides entirely in a random delay τ. Thus

$$R(f) = e^{j2\pi f\tau} , \tag{15}$$

where τ is a random variable having probability density $p_\tau(\tau)$ and characteristic function $P_\tau(f)$,

$$P_\tau(f) = \overline{e^{-j2\pi f\tau}} . \tag{16}$$

Then we have the expressions

$$\overline{R^*(f)} = P_\tau(f) \tag{17}$$

$$\overline{|R(f)|^2} = 1 \tag{18}$$

and

$$\overline{R^*(f)\, R(f - \tfrac{k}{T}) = e^{-j2\pi \frac{k}{T}\tau}} = P_\tau(\tfrac{k}{T}). \tag{19}$$

If we further assume that $N(f) \approx 0$, the high signal-to-noise ratio case then for $f > 0$, $W(f)$ becomes

$$W(f) = \begin{cases} \tau P_\tau(f) & , \quad 0 < f < \frac{1-\lambda}{2T} \\ \tau \dfrac{P_\tau(f) - P_\tau(f - \frac{1}{T})\, P_\tau(\frac{1}{T})}{1 - \left|P_\tau(\frac{1}{T})\right|^2} & , \quad \frac{1-\lambda}{2T} < f < \frac{1+\lambda}{2T}. \end{cases} \tag{20}$$

This $W(f)$ is shown in Fig. 2 for small random delay and coincides with previous results.[7,8]

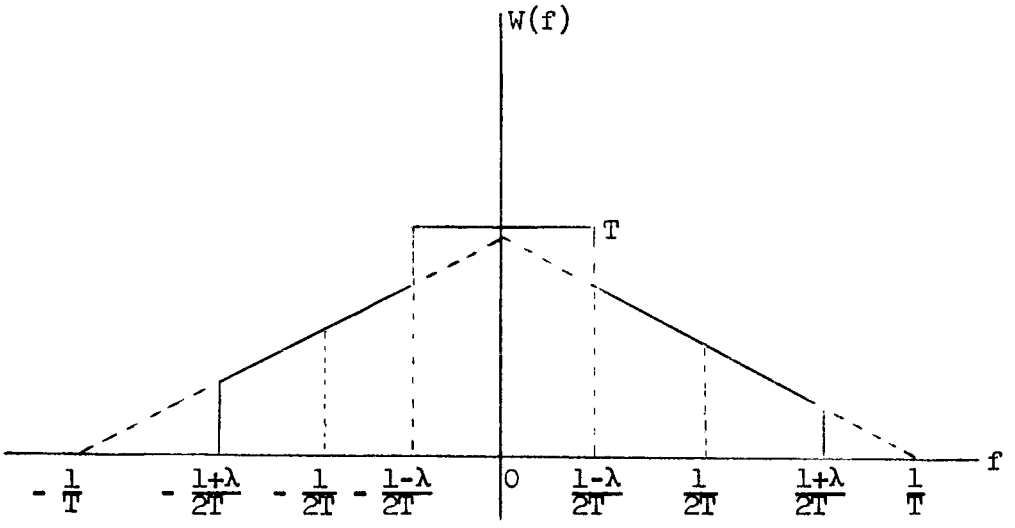


Fig. 2 Optimum Filter for Small Random Delay

Application to Random Phase and Random Delay in PAM-AM

Let us nos assume that the received pulse shape $r(t)$ is a randomly-delayed (by τ seconds) baseband pulse produced by synchronous demodulation of a passband pulse with Fourier transform $Z(f)$. We assume that the fractional phase $x = \theta/2\pi$ of the demodulating oscillator is a random variable having probability density $q_x(x)$ and characteristic function $Q_x(f)$. Thus $R(f)$ is

$$R(f) = \begin{cases} \left[e^{j2\pi x} Z(f_c - f) + e^{-j2\pi x} Z(f_c + f) \right] e^{j2\pi f\tau}, & |f| < W \\ 0, & |f| > W, \end{cases} \tag{21}$$

where the random variable τ has $p_\tau(\tau)$ and $P_\tau(f)$, as before. The generation and demodulation of the passband pulse $z(t)$ are depicted in Fig. 3. This is the channel model for a PAM-AM system.

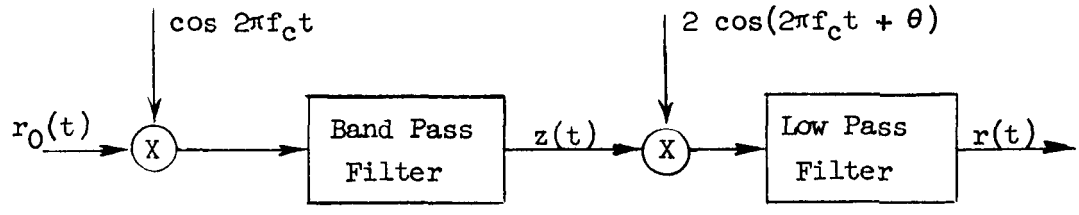


Fig. 3 Generation and Demodulation of $z(t)$

We assume in connection with (21) and Fig. 3 that $r_0(t)$ contains no energy in the frequency band $|f| > W$ and that the low pass filter cut-off

frequency W satisfies

$$W = \frac{1+\lambda}{2T} < f_c. \tag{22}$$

Then using the procedure outlined in the previous section we can solve for W(f). Using this W(f) and assuming 1) that θ and τ are statistically independent and 2) that N(f) = 0, the high-signal-to-noise ratio case, we calculate the resulting A_{min} to be

$$A_{min} = 1 - 2\,T\,Q_x(1)\,2\int_0^{\frac{1-\lambda}{2T}} |P_\tau(f)|^2 df$$

$$- \frac{2T|Q_x(1)|^2}{1 - P_\tau(\frac{1}{T})|Q_x(-2)|^2} \int_{\frac{1-\lambda}{2T}}^{\frac{1+\lambda}{2T}} P_\tau^*(f)\left[P_\tau(f) - P_\tau^*(\tfrac{1}{T} - f)\,Q_x(-2)\,P_\tau(\tfrac{1}{T})\right] df. \tag{23}$$

We have evaluated the A_{min} of Equation (23) for x and τ uniformly distributed over $(-x_0, x_0)$ and $(-\tau_0, \tau_0)$ respectively, and for several values of λ, the excess bandwidth. The results are shown in Fig. 4 and show explicitly the trade-offs between the three parameters x_0, τ_0, and λ.

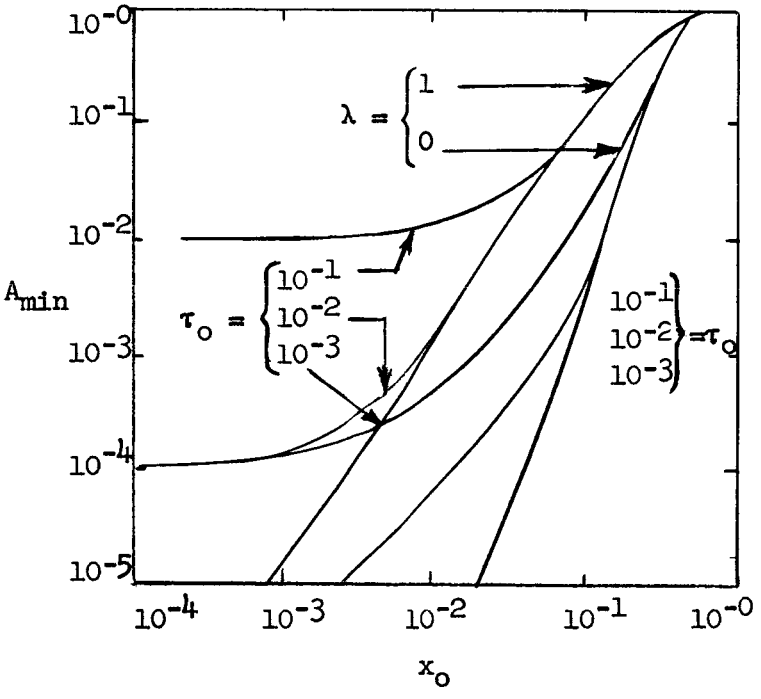


Fig. 4 A_{min} Versus Maximum Phase Jitter, x_o, for Various Excess Bandwidth, λ, and Maximum Timing Jitter, τ_o

Conclusion

We have specified the linear, time-invariant equalizer, $W(f)$, which minimizes the mean-square error in a digital system using PAM through a randomly selected channel, $R(f)$. The equalizer is specified in terms of the average transmission, $\overline{R(f)}$, the (frequency) autocorrelation function, $\overline{R^*(f)\, R(\ell)}$, the message power spectrum $M(f)$ and the noise power spectrum $N(f)$.

The solution for $W(f)$ has been demonstrated for the bandlimited case where the available (double-sided) bandwidth is less than twice the pulsing rate of $\frac{1}{T}$ pulses per second. We elaborate upon this solution to show the trade-offs between bandwidth, timing errors and phase errors in a PAM-AM system.

REFERENCES

1. R. W. Lucky, "Automatic Equalization for Digital Communication", BSTJ, April 1965, pp. 547-588.

2. M. J. DiToro, "A New Method of High Speed Adaptive Serial Communication through any Time-Variable and Dispersive Transmission Medium", Conference Record of First IEEE Annual Communications Symposium, Boulder, Colorado; June 7-9, 1965.

3. D. W. Tufts, "Nyquist's Problem - The Joint Optimization of Transmitter and Receiver in Pulse Amplitude Modulation", Proc. IEEE, Vol. 53, pp. 248-259, March 1965.

4. M. R. Aaron and D. W. Tufts, "Intersymbol Interference and Error Probability", IEEE Transactions on Information Theory, Vol. IT-12, pp. 26-35, January 1966.

5. D. W. Tufts, "Certain Results in Pulse Transmission Theory", Tech. Rep. 355, Cruft Laboratory, Harvard University, February 5, 1962.

6. T. Berger and D. W. Tufts, "Optimum Pulse Amplitude Modulation Part I: Transmitter-Receiver Results and Bounds from Information Theory", to be published IEEE Transactions on Information Theory, April 1967.

7. L. E. Franks, "Further Results on Nyquist's Problem in Pulse Transmission", unpublished Bell Telephone Laboratories Memorandum, May 10, 1966.

8. D. W. Tufts and T. Berger, "Optimum Pulse Amplitude Modulation Part II: Inclusion of Timing Jitter", accepted for publication, IEEE Transactions on Information Theory.

9. F. K. Becker, E. R. Kretzmer, and J. R. Sheehan, "A New Signal Format for Efficient Data Transmission", BSTJ , Vol. XLV, pp. 755-758, May - June 1966.

10. E. R. Kretzmer, "Generalization of a Technique for Binary Data Communication", IEEE Transactions on Communication Technology, pp. 67-68, February 1966.

11. R. D. Howson, "An Analysis of the Capabilities of Poly-binary Data Transmission", IEEE Transactions on Communication Technology, pp. 312-319, September 1965.

12. A. Lender, "Correlative Level Coding for Binary Data Transmission", IEEE Spectrum 3, pp. 104-115, February 1966.

13. D. W. Tufts and C. V. Ramamoorthy, "Modulo-m Linear Sequential Circuits, Partial Response Signaling Formats, and Signal Flow Graphs", (submitted for publication IEEE Transactions on Information Theory).

PART II SUMMARIES OF SCIENTIFIC REPORTS

CHAPTER I

SCIENTIFIC REPORT NO. 1

PULSE SHAPING BY MANIPULATING TRANSFORM ZEROS

J. B. Campbell
S. H. Chang
D. W. Fermental
N. T. Tsao-Wu

The treatments of pulse design problems in recent papers directly or indirectly make use of Fourier transform properties established in the theory of entire functions. The basic property used is that since it is an entire function of exponential type[1], the Fourier transform of a pulse possesses and is characterized by an infinite set of zeros in the complex frequency plane.[2] Pulse design can be effected by operations on these zeros, as indicated in recent papers.

The possibility of a transform zero canceling a system function pole, was used by Gerst and Diamond[3] to design signal inputs to a system to yield pulse outputs for the elimination of intersymbol interference. They have discussed the following problem. Given a time-invariant, linear system, find an input such that the output is a pulse. They show that in the lumped-element (and in certain cases, transmission line type) systems, it is possible to have both input and output as pulses, and that this is effected when the poles of the system function are canceled by zeros of the transform of a pulse. In their equivalent time-domain solution, Gerst and Diamond show that differentiable pulses can be valuable design tools.

In an extension by Campbell[4] of the Gerst and Diamond work, differentiable pulses are used to design pulse inputs that correspond to a set of orthogonal pulse outputs of a given system.

As pointed out by Hofstetter[5] and Walther[6], a pulse is uniquely determined by its energy density spectrum if the zeros of the spectrum function all lie on the real axis of the complex frequency plane. Given a pulse whose Fourier transform has zeros in the upper-half (lowér-half) frequency plane, Hofstetter and Walther have shown that "flipping" of zeros to the lower-half (upper-half) plane can be used to find a set of pulses with the same autocorrelation function (or energy density spectrum).

In solving a related problem[7] Fermental has shown that, under certain conditions, transform zeros can be "flipped" to obtain a set of orthogonal pulses with the same energy density spectrum.

This report presents an investigation into the effect produced on a pulse by manipulating its transform zeros. In particular, zero manipulations for the folowing purposes are discussed. (1) By removing transform zeros, a pulse is shaped to have more derivatives. The zero removal process is extended to yield an infinitely-differentiable pulse. (2) By zero deletion and shifting, a pulse is made to approximate a chosen waveform. (3) By zero deletion and shifting, a pulse is shaped to have: (a) a specified amplitude density spectrum (e.g., rectangular-pulse-like); or (b) a specified energy density spectrum (e.g., complementary to "colored" noise of the 1/f type).

REFERENCES

1. R.E.A.C. Paley and N. Wiener, "Fourier Transforms in the Complex Domain", American Mathematical Society Colloquium Publications, Vol. XIX, 1934, Theorem X, p. 13.

2. B. Ja. Levin, "Distribution of Zeros of Entire Functions", Translations of Mathematical Monographs, Vol. 5, American Mathematical Society, 1964, Theorem 11, p. 251.

3. I. Gerst and J. Diamond, "The Elimination of Intersymbol Interference by Input Signal Shaping", Proc. I.R.E., Vol. 49, No. 7, July 1961, pp. 1195-1203.

4. J. B. Campbell, F. B. Reis, "The Design of Input Waveforms to Yield Time-Limited Orthogonal Outputs", Scientific Report No. 3, for Contract No. AF19(604)-7494 and Grant No. AF-AFOSR-62-371, Northeastern University, March 1963.

5. E. M. Hofstetter, "Construction of Time-Limited Functions with Specified Autocorrelation Functions", IEEE Transactions on Information Theory, Vol. IT-10, April 1964, pp. 119-126.

6. A. Walther, "The Question of Phase Retrieval in Optics", Optica Acta, Vol. X, No. 1, January 1963, p. 41.

7. D. W. Fermental, "Construction of Orthogonal Pulses with the Same Autocorrelation", 1965 IEEE Convention Record.

CHAPTER II

SCIENTIFIC REPORT NO. 2

PROPERTIES AND APPLICATIONS OF AUTOCORRELATION-INVARIANT FUNCTIONS

R. A. Gonsalves

This work resulted as a by-product of a research effort to find a set of orthogonal time functions, non-zero only for $t > 0$, which have the same autocorrelation function. Such a set is the set of Laguerre functions whose first few members are

$$e^{-t/2}, \quad t > 0$$

$$e^{-t/2}(1-t), \quad t > 0$$

$$e^{-t/2}\left(1 - 2t + \frac{t^2}{2}\right), \quad t > 0.$$

Each member of this set has an autocorrelation function which is

$$e^{-\left|\frac{\tau}{2}\right|}.$$

Note that the first member of the set of Laguerre functions has exactly the same form as its autocorrelation function for t (or τ) > 0. Such a time function $f_N(t)$ whose autocorrelation function is $f_N(|\tau|)$ is called Autocorrelation-Invariant (A-I); that is, $f_N(t)$ is invariant under the operation of autocorrelation. The study of the class of A-I functions is the subject of this report.

It is shown that A-I functions have several properties of interest to the communications engineer. These include:

(a) $f_N(t)$ is the right half of an ACF, providing a simple sufficiency test for a specified function to be an ACF.

(b) Associated with $f_N(t)$ and generated in the manner of the Laguerre functions, is an orthogonal set whose members are useful as basis functions in the design of orthogonal signalling waveforms with specified ACF's.

(c) $f_N(t+\tau)$ is the degenerate kernel of an integral equation whose N+1 eigenvalues are real and unity in magnitude, and whose eigenfunctions span $\mathcal{F}_N$, a finite-dimensional subspace of Hilbert space. This property allows several results in the characterization of time functions in $\mathcal{F}_N$.

The Laguerre and Legendre functions of the first kind, two sets of A-I functions, are defined and discussed. A curious orthogonality property of any member of the former set, under time translations, is presented, giving rise to a conjecture concerning all A-I functions.

CHAPTER III

SCIENTIFIC REPORT NO. 3

ORTHOGONAL SIGNALLING PULSES WITH THE SAME AUTOCORRELATION

Denis W. Fermental

A problem of some interest to communication engineers is the simultaneous transmission of orthogonal pulses having the same duration with independent detection at a receiver by matched filtering and sampling. A question that arises naturally in this connection is, how closely can such pulses be alike in bandwidth? In this report a method is developed by which orthogonal pulses can be constructed with identical bandwidths. More precisely, these pulses have the same energy density spectrum. The technique consists of forming linear combinations of some sufficiently differentiable pulse and its derivatives to generate the required waveforms. The report determines criteria for the coefficients of these linear combinations and shows that the restrictions on the sufficiently differentiable pulse may be expressed in terms of the moments of its energy density spectrum.

To clarify the approach which is adopted, we examine the following special case. Let the pulse $g(t)$ have a bounded derivative $g'(t)$. Then for any real number α, the pulses

$$f_0(t) = g'(t) + \alpha g(t)$$

$$f_1(t) = g'(t) - \alpha g(t)$$

have the same energy density spectrum, $\Phi_f(\omega)$ which is

$$\Phi_f(\omega) = (\omega^2 + \alpha^2)\, \Phi_f(\omega),$$

where $\Phi_g(\omega)$ is the energy density spectrum of $g(t)$.

For $f_0(t)$ and $f_1(t)$ to be orthogonal we must also require that

$$\int_{-\infty}^{\infty}[g'(t) - \alpha g(t)][g'(t) + \alpha g(t)]\,dt =$$

$$\int_{-\infty}^{\infty}[g'(t)]^2\,dt - \alpha^2\int_{-\infty}^{\infty}[g(t)]^2\,dt = 0.$$

By Parseval's theorem

$$\int_{-\infty}^{\infty}[g(t)]^2\,dt = \frac{1}{2\pi}\int_{-\infty}^{\infty}\Phi\ (\omega)\,d\omega = \frac{u_0}{2\pi}$$

and

$$\int_{-\infty}^{\infty}[g'(t)]^2\,dt = \frac{1}{2\pi}\int_{-\infty}^{\infty}\omega^2\ \Phi_g(\omega)\,d\omega = \frac{u_2}{2\pi}\ .$$

Then for orthogonality

$$\alpha = \frac{u_2}{u_0}\ ,$$

where u_0 and u_2 are the zeroth order moment and the second order moment of $\Phi_g(\omega)$. The two pulses

$$f_0(t) = g'(t) + \frac{u_2}{u_0}\,g(t)$$

$$f_1(t) = g'(t) - \frac{u_2}{u_0}\,g(t)$$

are, therefore, orthogonal and have the same autocorrelation function. Here α was determined by the moments of the given $\Phi_g(\omega)$. We could, however, choose an appropriate α and thus place a restraint on the moments

if some $\Phi_g(\omega)$ to be constructed later. This is the approach that is adopted in this report.

By taking into consideration the properties of sufficiently differentiable pulses (time-limited or finite support) and making use of the method of moments of the energy spectrum, the reports shows that it is possible to construct a set of real pulses with three properties:

(a) the pulses have the same support,

(b) the pulses are mutually orthogonal over this support,

(c) the pulses have the same autocorrelation function, or equivalently, the same energy density spectrum.

CHAPTER IV

ABSTRACT OF SCIENTIFIC REPORT NO. 4

ON LINEAR PRODUCT CODES AND THEIR DUALS

L. J. Weng

In this report the value of studying the tensor product of linear codes, the iterated codes and the error-locating codes, is demonstrated. The pertinent problems concerning these product codes are outlined.

One of the important problems is to relate both the code space and its null space of a tensor product code to the code spaces and null spaces of the component codes of the product code. An extensive study in this area is given in the report. First a brute-force and tedious direct approach is illustrated. A more meaningful algebraic approach is then developed. The result can be expressed in various forms; each of them gives a special interpretation. A better insight of the product code structure is thus obtained. The determination of null space of a tensor product space involving the translation of fields is also treated. In this case the elements of two original component codes and elements of the resultant product code are expressed in different fields. The result shows that this will give us more efficient error-locating codes. But no advantage will be obtained by constructing iterated codes through fields translation.

The problem of encoding and decoding of tensor product codes are considered in detail. Decomposition of the procedure and implementation of encoding and decoding of a product code into those of its component

codes is emphasized. The general encoding and decoding schemes applicable to all product codes are first studied. Then special attention is given to the product codes whose component codes are cyclic. Since the implementation of cyclic codes can be achieved easily by linear shift-registers and the encoder can be converted to that of its dual code by varying the input and output positions, the encoder of an iterated code or an error-locating code can possess four operating modes by converting one, one, or both of its component codes to their respectively dual codes.

Furthermore, the report shows that the encoding circuit of an iterated code and that of an error-locating code are very similar if their component codes are the same. Therefore, it is possible to implement an eight mode encoder -- 4 high-redundancy iterated codes and 4 low-redundancy codes. The encoder can be converted to a syndrome calculator for any of the eight product codes. A simple decoding scheme, namely permutation decoding, which is capable of correcting a large fraction of all correctable errors of a systematic cyclic code, is investigated. It is suggested that it be used either as a part of the correction-detection scheme or in combination with an auxiliary scheme to attain full error correction capability. Finally, the minimum distances of both iterated codes and error-locating codes, and suitable communication channels for employing such codes, are discussed.

CHAPTER V

SCIENTIFIC REPORT NO. 5

IMPLEMENTATION AND PERFORMANCE OF THE MAXIMUM-LIKELIHOOD DETECTOR IN A CHANNEL WITH INTERSYMBOL INTERFERENCE

R. A. Gonsalves

High speed data communication via PAM requires the simultaneous control of intersymbol interference (ISI) and random noise. In this report we give an explicit structure for the maximum-likelihood (ML) receiver which accomplishes this purpose. The receiver is optimum in the sense that it minimizes the per-symbol probability of error, P_e. The non-linear structure contains elements of the optimum linear receiver and the decision feedback (or "tail cancellation") receiver.

We assume independent, binary (± 1) data, a known signalling pulse shape $s(t)$ which lasts for two bauds (giving rise to limited ISI), stationary additive, white (power spectral density = $N_o/2$), Gaussian noise, and perfect synchronism between transmitter and receiver. Several of these assumptions can be removed by more complex analyses; perhaps the most bothersome, the assumption of limited ISI, is removed here only by a heuristic argument.

The ML receiver processes as much of the received data $y(t)$ as is available, producing a statistic λ_k to decide on the polarity of the k^{th} bit, μ_k. λ_k is given by

$$\lambda_k = A_k + Z\{A_{k-1} + Z\{A_{k-2} + \cdots\}\} + Z\{A_{k+1} + Z\{A_{k+2} + \cdots\}\} , \qquad (1)$$

where A_k is a correlation statistic given by

$$A_k = \frac{4}{N_o}\int y(t)\, s(t-kT)\, dt, \tag{2}$$

$$Z\{x\} = \log_e \frac{e^x + e^R}{1 + e^{x+R}}, \tag{3}$$

and

$$R = \frac{4}{N_o}\int s(t)\, s(t+T)\, dt. \tag{4}$$

These equations are implemented in Fig. 1. The input-output characteristic of the non-linear device defined by Equation (3) is shown in Fig. 2 for several values of the ISI parameter R.

Fig. 1 points up the similarity between the ML receiver and the optimum linear receiver that is, a matched filter followed by a tapped delay line. In this structure, however, the useful output is a non-linear rather than a linear sum of the tap outputs.

Upper and lower bounds on P_e have been set and a sample curve is presented showing P_e versus SNR. This curve shows that the detector compares favorably with several other detection schemes at all SNR.

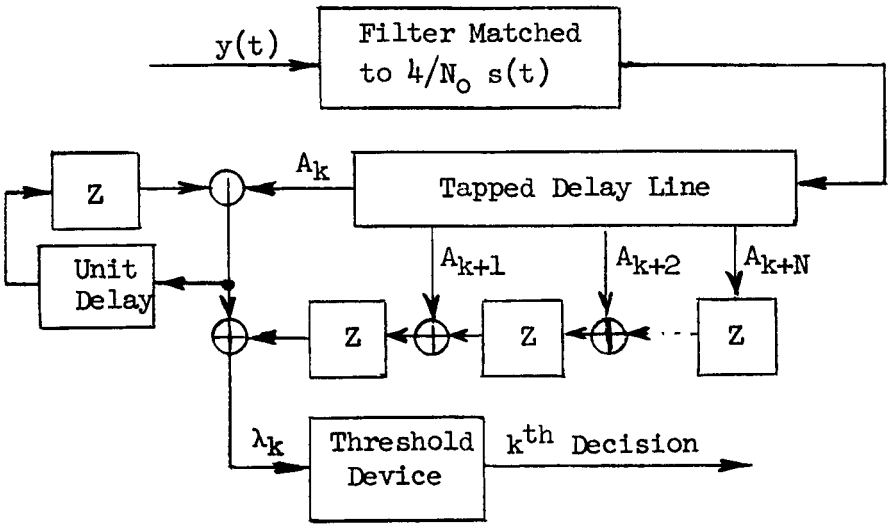


Fig. 1 The ML Receiver

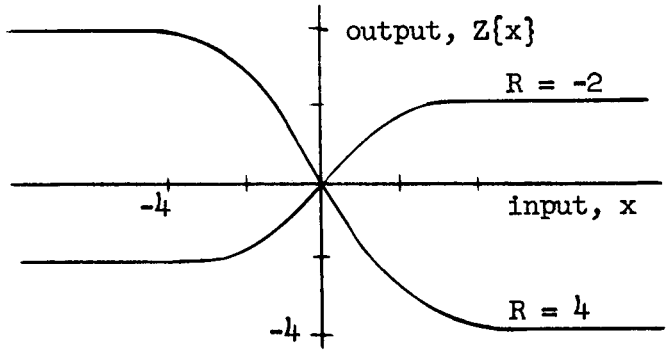


Fig. 2 Non-Linear Characteristics of Z{x}

CHAPTER VI

COMMUNICATION THEORY GROUP REPORT NO. 6

OPTIMUM INTERPOLATION OF SAMPLED FUNCTIONS

M. Schetzen

A study of optimum sampling and interpolation of random processes was begun under this contract. The results of the first part of the initial study, optimum linear interpolation, is presented in this report.

The problem derives its importance from the fact that many information processing systems sample the data being processed. The desired function must then be reconstructed from the sampled data. Examples of such systems used in communications are pulse and delta modulators; digital systems also require the data being processed to be sampled. Often, the data is reconstructed by means of a low-pass R-C filter; sometimes a zero- or first-order hold circuit is used. The waveform reconstructed by these techniques closely approximates the sampled function if the sampling rate is large as compared with the bandwidth of the function being sampled and if the sampled data is accurate so that it is not corrupted by very much noise. For a given error criterion, it is clear that these interpolation procedures are generally not optimum.

In the ideal case of a time function $f(t)$ whose spectrum is zero for $\omega > 2\pi f_m$, it is known that it can be reconstructed with zero error from a set of equally spaced sampled data in which the sampling rate, $\frac{1}{T_1}$, is

greater than $2f_m$. The interpolation is

$$f(t) = 2T_1 f_m \sum_{n=-\infty}^{\infty} f(nT_1) \frac{\text{Sin } 2\pi f_m(t-nT_1)}{2\pi f_m(t-nT_1)}$$

in which T_1 is the spacing between samples.

This interpolation formula is not physically realizable since the interpolated value of f(t) depends upon the samples f(nT) for $nT > t$. By increasing the sampling rate so that it is greater than $6f_m$, f(t) can be interpolated in terms of only the samples f(nT) for $nT \leq t$.[2] In all practical cases, however, a message is not completely determined by its own past. If it were so determined, then at no period in the message would it be possible to introduce new information. Thus bandlimited functions are in a certain sense "singular".[3] If a random function, f(t), is not singular, then it cannot be interpolated with zero mean-square error on the basis of its past samples, f(nT) for $nT \leq t$. The problem of determining the optimum causal interpolation function and the minimum obtainable error thus is significant.

For periodic sampling, explicit expressions of the optimum causal linear interpolation filter for the interpolation of corrupted samples are presented in the report. The criterion used was that the mean-square error be a minimum. In addition, expressions for the minimum mean-square error are obtained. These results, which are believed to be new, are illustrated by some specific examples of practical importance. In order to study the properties of the waveform that contribute to the error, simple bounds of the irremovable error were obtained. As an example, for the important case in which the power density spectrum of the random process

is a strictly monotonically decreasing function of frequency, it is shown that the irremovable mean-square error lies between one and two times the power in the random process above one-half the sampling frequency. This bound implies that, in choosing a sampling frequency, it is the power in the "tails" of the spectrum and not the amplitude of the spectrum that should be considered.

The second part of this initial study, optimum pre-emphasis, is in progress. In addition to optimum pre-emphasis systems, the minimum error as a function of the average sampling rate for various efficient sampling procedures will be studied.

REFERENCES

1. E. T. Whittaker, "On the Functions which are Represented by the Exapnsions of the Interpolation Theory", Proc. Royal Society, Edinburgh, Vol. 35, (1915), pp. 181-194.

2. Wainstein and Zubakov, Extraction of Signals from Noise, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1962.

3. Kolmogoroff, "Interpolation und extrapolation von stationären zufälligen Folgen", Bulletin de L'académie des sciences de U.S.S.R., Ser. Math. 5, 1941.

CHAPTER VII

COMMUNICATION THEORY GROUP REPORT NO. 7

A STUDY OF ADAPTIVE BANDWIDTH COMPRESSION*

L. Ehrman

The performance characteristics of four adaptive bandwidth compression techniques - the floating-aperture predictor, the zero-order interpolator, the fan interpolator and the maximum length interpolator - are found in analytic form. It is shown that the mean and mean-square time between output samples are, for a floating-aperture predictor with vector Markov process input signals, the solutions of two integral equations whose kernels are the conditional probability density function of the input process, while for a zero-order interpolator and a maximum length interpolator they can be expressed as space-time integrals of the input signal's range and adjusted range probability density function. The mean and mean-square output times of the fan interpolator are expressed as the sum of iterated integrals of the signal's conditional probability density function over the aperture space.

The relation between peak error and RMS error is derived for each compression algorithm. The transmission bandwidth required for each algorithm is found for the case when the input signal is a first-order Gauss-Markov process. This bandwidth is compared with that required for

---

*This report is based on a Ph.D. thesis written under a National Science Foundation Fellowship. The writer was affiliated with the Communication Theory Group while preparing the thesis.

uniformly sampled data which is reconstructed by means of the optimum time-invariant linear interpolator filter. It is shown that the fan interpolator requires approximately the same bandwidth as does the optimum filter, while the floating-aperture predictor requires about 2.5 times the bandwidth. The zero-order interpolator falls midway between the floating-aperture predictor and the fan interpolator in performance. The maximum length interpolator is superior only to the floating-aperture predictor; it is surmised that this behavior is a characteristic of disjoint interpolators, in general.

LIST OF PUBLICATIONS

Scientific Report No. 1, December 1964 (AFCRL-65-20)

"Pulse Shaping by Manipulating Transform Zeros", by J. B. Campbell, S. H. Chang, D. W. Fermental and N. T. Tsao-Wu.

Scientific Report No. 2, June 1965 (AFCRL-65-427)

"Properties and Applications of Autocorrelation-Invariant Functions", by Robert A. Gonsalves, (based on a Ph.D. thesis).

Scientific Report No. 3, June 1965 (AFCRL-65-462)

"Orthogonal Signalling Pulses with the Same Autocorrelation", by Denis W. Fermental, (based on a Ph.D. thesis).

Scientific Report No. 4, June 1966 (AFCRL-66-471)

"On Linear Product Codes and Their Duals", by Lih-Jyh Weng, (based on a Ph.D. thesis).

Scientific Report No. 5, August 1966 (AFCRL-66-586)

"Implementation and Performance of the Maximum-Likelihood Detector in a Channel with Intersymbol Interference", by Robert A. Gonsalves.

Communication Theory Group Report No. 6

"Optimum Interpolation of Sampled Functions", by Martin Schetzen.

Communication Theory Group Report No. 7

"A Study of Adaptive Bandwidth Compression", by Leonard Ehrman. (A report based on a Ph.D. thesis written under a National Science Foundation Fellowship. The writer was affiliated with the Communication Theory Group while preparing this thesis.)

Two Technical Papers - presented at the 1965 International Convention of IEEE, March 22-26, 1965, New York, New York.

"Error-Locating Codes", by S. H. Chang and L. J. Weng.

"Construction of Orthogonal Pulses with the Same Autocorrelation", by D. W. Fermental.

A Technical Paper - presented at the Symposium on Models for Perception of Speech and Visual Forms, sponsored by AFCRL, and held at Boston, Massachusetts on November 11-14, 1964.

"A Criterion for the Selection for Speech Features in Speech Recognition Based on Comparison of Experiments", by D. C. Lai.

A Technical Paper - presented at the Symposium on Signal Transmissions and Processing, at Columbia University, New York, New York, May 13, 1965.

"Pulse Shaping by Manipulating Transform Zeros", by J. B. Campbell, S. H. Chang, D. W. Fermental, N. T. Tsao-Wu.

A Technical Paper - presented at the First IEEE Annual Communication Convention, at Boulder, Colorado on June 7-9, 1965.

"Laguerre Functions of the First Kind in Signal Design and Representation", by R. A. Gonsalves.

A Technical Paper - presented at the IEEE International Symposium on Information Theory, at UCLA, Los Angeles, California, on January 31 - February 3, 1966.

"Dual Product Codes", by S. H. Chang and L. J. Weng.

A Technical Paper - presented at the IEEE International Communication Conference, Philadelphia, Pennsylvania on July 15-17, 1966.

"A Note on Non-binary Orthogonal Codes", by S. H. Chang.

A Technical Correspondence - accepted for publication in the IEEE Transactions of Professional Group on Information Theory.

"Discussion on Arithmetic Codes with Large Distance", by S. H. Chang and N. T. Tsao-Wu.

Two Technical Papers - accepted for presentation at the forthcoming 1967 IEEE International Conference on Communication, Minneapolis, Minnesota, June 12-14, 1967.

"Variable Redundancy Product Codes", by L. J. Weng and G. H. Sollman.

"Maximum-Likelihood Receiver for Digital Data Transmission", by R. A. Gonsalves.

A Master's Thesis, March 1965

"Pulse Shaping by Linear Networks", by Nelson T. Tsao-Wu.

A Master's Thesis, May 1966

"A Study of Shape Recognition Using the Medial Axis Transformations", by Otis Philbrick.

A Master's Thesis, March 1967

"The Implementation and Application of a Product Encoder with Variable Modes of Redundancy", by George Sollman.

DISTRIBUTION LIST

Arizona State College
Post Office Box 942
Flagstaff, Arizona
ATTN: Prof. A. Adel

The Johns Hopkins University
Lab of Astrophysics & Phys. Meteor.
Baltimore, Maryland
ATTN: Dr. William S. Benedict

IDA
400 Army-Navy Drive
Arlington, Virginia 22302
ATTN: Lucien M. Biberman

Meteorologisches Institut Der
Universitat Munchen
Amalienser. 52/111
8000 Munchen 13 Germany
ATTN: Dr. H. J. Bolle

Environmental Science Services Adm.
Boulder, Colorado 80302
ATTN: R. F. Calfee

APGC (PGVER)
Eglin Air Force Base, Florida 32542
ATTN: D. Cavitch

General Electric Company
Space Science Laboratory
Philadelphia, Pennsylvania
ATTN: Dr. K. L. Coulsen

Canadian Armament R & Destablishment
Post Office Box 1427
Valcartier, Quebec, Canada
ATTN: Dr. Cameron Cumming

Research Activities Building
North Campus
Ann Arbor, Michigan 48105
ATTN: S. Roland Drayson

EMI Electronics Ltd.
Infrared Research Department
Victoria Road
Falthem, Middlesex, England
ATTN: C. B. Farmer

AFCRL (CRO) Stop 30
L. G. Hanscom Field
Bedford, Massachusetts 01730
ATTN: Dr. J. S. Garing

Harvard University
Pierce Hall
Oxford Street
Cambridge, Massachusetts
ATTN: Dr. Richard Goody

University of Florida
Department of Physics
Gainsville, Florida
ATTN: Dr. A. Green

NASA-Goddard Space Flight Center
Greenbelt, Maryland
ATTN: R. A. Hanel

CCA Corporation
Burlington Road
Bedford, Massachusetts 01730
ATTN: Dr. J. I. F. King

Technical Operations Research
South Avenue
Burlington, Massachusetts 01803
ATTN: Dr. Irving L. Kofsky

University of Colorado
Department of Astro-Geophysics
Boulder, Colorado 80302
ATTN: Prof. Julius London

General Dynamics/ Convair
Department 596-2
5001 Kerney Villa Road
San Diego, California 92112
ATTN: Dr. C. B. Ludwig

University of Liege
Institute of Astrophysics
Cointe-Sciessin, Belgium
ATTN: Prof. M. V. Migeotte

Denver University
Physics Department
Denver, Colorado 80210
ATTN: David G. Murcray

Lockheed Missile & Space Company
Sunnyvale, California
ATTN: G. OPPEL

Smithsonian Institute
Astrophysical Observatory
60 Garden Street
Cambridge, Massachusetts
ATTN: Carl Sagan

The Johns Hopkins University
Lab of Astrophysics & Phys. Meteor.
Baltimore, Maryland
ATTN: Prof. John Strong

Southwestern At Memphis
Physics Department
Memphis, Tennessee
ATTN: Prof. J. H. Taylor

Environmental Science Services Adm.
National Environmental Satellite
Center - FOB #4
Washington, D. C. 20233
ATTN: Dr. David Q. Wark

Kansas State University
Manhattan, Kansas
ATTN: Dr. Dudley Williams

Tohoku University
Geophysical Inst. - Faculty of Science
Sandal, Japan
ATTN: Prof. Gilchi Yamamoto

Block Engineering, Inc.
19 Blackstone Street
Cambridge, Massachusetts 02139
ATTN: A. S. Zachor

Polytechnic Institute of Brooklyn
Graduate Center - Route 110
Farnindale, Long Island
New York 11735
ATTN: Dr. Ralph Zirkind

Hq., AFCRL, OAR (CRBK) Stop 30
L. G. Hanscom Field
Bedford, Massachusetts 01730
ATTN: Charles F. Hobbs

AFCRL (CRMXLR) Stop 29
L. G. Hanscom Field
Bedford, Massachusetts 01730

AFCRL (CRMXLR) Stop 29
L. G. Hanscom Field
Bedford, Massachusetts 01730
ATTN: Mrs. Cora Gibson

AFCRL (CRMXRA) Stop 39
L. G. Hanscom Field
Bedford, Massachusetts 01730

AFCRL (CRMXRD) Stop 30
L. G. Hanscom Field
Bedford, Massachusetts 01730

AFCRL (CRN) Stop 30
L. G. Hanscom Field
Bedford, Massachusetts 01730

AFCRL (CRTE) Stop 30
L. G. Hanscom Field
Bedford, Massachusetts 01730

AFCRL (CRTPM) Stop 30
L. G. Hanscom Field
Bedford, Massachusetts 01730

ADC
Operations Analysis Office
Ent. Air Force Base
Colorado 80912

AFAL (AVX)
Wright-Patterson Air Force Base
Ohio 45433

AFETR
Technical Library-Mu-135
Patrick Air Force Base
Florida 32925

AFIT (MCLI, Library)
Building 640 - Area B
Wright-Patterson Air Force Base
Ohio 45433

AFSC-STLO (RSTAL)
AF Unit Post Office
Los Angeles, California 90045

AFSC-STLO (RTSAB)
Waltham Federal Center
424 Trapelo Road
Waltham, Massachusetts 02154

AFSC-STLO (RTSUM)
68 Albany Street
Cambridge, Massachusetts 02139

AFWL (WLIL)
Kirtland Air Force Base
New Mexico 87117

Dir., Air University Library
Maxwell Air Force Base
Alabama 36112
ATTN: AUL3T

APGC (PGBPS-12)
Englin Air Force Base
Florida 32542

OAR (RRY)
1400 Wilson Boulevard
Arlington, Virginia 22209

RADC (EMTLD)
Griffiss Air Force Base
New York 13440
ATTN: Documents Library

RTD
Scientific Director
Bolling Air Force Base
Washington, D. C.

SAC (OA)
Offutt Air Force Base
Nebraska 68113

Systems Engineering Group (RTD)
Wright-Patterson Air Force Base
Ohio 45433
ATTN: SEPIR

SSD (SSTRT)
Los Angeles Air Force Station
AFUPO
Los Angeles, California 90045
ATTN: Lt. O'Brien

Hq., TAC (OA)
Langley Air Force Base
Virginia 23362

USAF Academy
Academy Library (DFSLB)
Colorado 80840

Army Missle Command
Redstone Scientific Info. Center
Redstone Arsenal, Alabama 35809
ATTN: Chief, Document Section

U. S. Army Electronics Command
Technical Document Center
Fort Monmouth, New Jersey 07703
ATTN: AMSEL-RD-MAT

Chief of Naval Operations
(OP-413-B21)
Washington, D. C.

Naval Ordnance Laboratory
Technical Library
White Oak, Silver Spring
Maryland 20910

Commanding Officer
Office of Naval Research Branch Off.
Box 39 - Fleet Post Office
New York 09510

Director
Naval Research Laboratory
Washington, D. C. 20390
ATTN: 2027

U. S. Naval Ordnance Test Station
China Lake,California 93555
ATTN: Technical Library

U. S. Naval Postgraduate School
Library (Code 2124)
Monterey, California 93940

U. S. Navy Electronics Laboratory (Library)
San Diego, California 92152

Central Intelligence Agency
Washington, D. C. 20505
ATTN: OCR/DD/STD. Distribution

Clearinghouse for Federal Scientific
& Technical Information (CFSTI)
Sills Building
5285 Port Royal Road
Springfield, Virginia 22151

Director
Defense Atomic Support Agency
Washington, D. C. 20301
ATTN: Technical Library Section

Defense Documentation Center (DDC)
Cameron Station
Alexandria, Virginia 22314

DIA
(DIAAP-142)
Washington, D. C. 20301

Environmental Sciences Services Adm.
Library
Boulder Laboratories
Boulder, Colorado 80302

FAA
Bureau of Research & Development
300 Independence Avenue, S.W.
Washington, D. C. 20553

Government Printing Office
Library
Division of Public Documents
Washington, D. C. 20402

Library of Congress
Aerospace Technical Division
Washington, D. C. 20540

Library of Congress
Exchange & Gift Division
Washington, D. C. 20540

U. S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204
ATTN: Technical Library

NASA Scientific & Technical
Information Facility
Post Office Box 33
College Park, Maryland 20740
ATTN: Acquisitions Branch (S-AK/DL)

NASA-Flight Research Center
Library
Post Office Box 273
Edwards, California 93523

NASA-Goddard Inst. for Space Studies
(Library)
2880 Broadway
New York, New York 10025

NASA-Goddard Space Flight Center
Technical Library
Greenbelt, Maryland 20771

NAS-Jet Propulsion Laboratory
4800 Oak Grove Drive
Pasadena, California 91103
ATTN: Library (TDS)

NASA-Lewis Research Center
Library - Mail Stop 60-3
21000 Brookpark Road
Cleveland, Ohio

NASA-Manned Spacecraft Center
Technical Library
Houston, Texas 77058

National Center for Atmospheric
Research
NCAR Library, Acquisitions
Boulder, Colorado 80302

ODDR & E (Libary)
Room 3C-128
The Pentagon
Washington, D. C. 20301

AIAA-TIS Library
750 Third Avenue
New York, New York 10017

Aerospace Corporation
Post Office Box 95085
Los Angeles, California 90045
ATTN: Library Acquisitions Group

Battelle Memorial Institute
Library
505 King Avenue
Columbus, Ohio 43201

The Mitre Corporation
Post Office Box 208
Bedford, Massachusetts 01730
ATTN: Library

The Rand Corporation
1700 Main Street
Santa Monica, California 90406
ATTN: Library-D

British Defence Staffs
British Embassy
Scientific Information Officer
3100 Massachusetts Avenue, N.W.
Washington, D. C. 20008

Chief, Canadian Defence
Research Staff
2450 Massachusetts Avenue, N.W.
Washington, D. C. 20008
(Technical & Scientific Reports will be released for military purposes only and any proprietary rights which may be involved are protected by United States/United Kingdom & Canadian Government Agreements.)

National Research Council
National Science Library
Ottawa 7, Canada

General Electric Company
Military Comm. Department
4000 North West 39th Street
Oklahoma City, Oklahoma 73102
ATTN: M. E. Mitchell

Distribution List for NASA, ERC

ERC - Library
NASA, ERC
575 Technology Square
Cambridge, Massachusetts 02139

NASA, ERC
Systems Research Laboratory
Guidance and Control Branch
575 Technology Square
Cambridge, Massachusetts 02139
ATTN: Mr. Stephen J. O'Neil

NASA, ERC
Systems Research Laboratory
Guidance and Control Branch
575 Technology Square
Cambridge, Massachusetts 02139
ATTN: Mr. Jean Roy

Unclassified
Security Classification

DOCUMENT CONTROL DATA - R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)*: Northeastern University, Department of Electrical Engineering, 360 Huntington Avenue, Boston, Massachusetts 02115

2a. REPORT SECURITY CLASSIFICATION: Unclassified

2b. GROUP:

3. REPORT TITLE

STATISTICAL COMMUNICATION THEORY

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

Final Scientific Report, period covered 1 December 1963 thru 31 March 1967

5. AUTHOR(S) *(Last name, first name, initial)*

Communication Theory Group

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
April 1967	90	40

8a. CONTRACT OR GRANT NO.: AF19(628)-3312 NASA Grant NGR-22-011-013

b. PROJECT NO. & Task No.: 4610-03

c. DOD Element: 62405304

d. DOD Subelement - 674610

9a. ORIGINATOR'S REPORT NUMBER(S):

9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*: AFCRL-67-0272

10. AVAILABILITY/LIMITATION NOTICES

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

11. SUPPLEMENTARY NOTES: Partially supported by the National Aeronautics and Space Agency, Cambridge, Massachusetts

12. SPONSORING MILITARY ACTIVITY: Hq., AFCRL, OAR (CRB) United States Air Force, L.G. Hanscom Field Bedford, Massachusetts 01730

13. ABSTRACT

This report describes four current research efforts: arithmetic codes, non-binary orthogonal codes, error-correcting schemes, and filtering of PAM signals for a randomly selected channel. Seven Scientific Reports are summarized. The subject matter of these reports includes the following topics: linear product codes, detection of digital data, optimum interpolation of sampled functions, adaptive bandwidth compression, and the design and shaping of analog signals.

DD FORM 1 JAN 64 1473

Unclassified
Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Algebraic Codes Arithmetic Codes Non-binary Orthogonal Codes Product Codes Dual Codes Error-Control Random Channel Signal Design Adaptive Sampling						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization *(corporate author)* issuing the report.

2*a*. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2*b*. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year; or month, year. If more than one date appears on the report, use date of publication.

7*a*. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7*b*. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8*a*. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8*b*, 8*c*, & 8*d*. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9*a*. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9*b*. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers *(either by the originator or by the sponsor)*, also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through _____."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through _____."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through _____."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring *(paying for)* the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as *(TS)*, *(S)*, *(C)*, or *(U)*.

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, rules, and weights is optional.

GPO 886-551